Галия Ибрагимова

СТРАТЕГИЯ КНР В ОБЛАСТИ УПРАВЛЕНИЯ ИНТЕРНЕТОМ И ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Китайский стратег и мыслитель Сунь Цзы в своем знаменитом трактате *Искусство войны* выразил главную идею китайской стратегии — *воевать без оружия, побеждать без боя*[1]. Несмотря на прошедшие лета и столетия, мудрость не утратила актуальность. Ведущие мировые державы стремятся вести противостояния с противником бескровными методами, а вместо оружия все чаще используют информационные технологии и ресурсы. Но *пальму первенства* в информационной войне уверенно сохраняет Китай. Об этом свидетельствуют данные и отчеты различных международных и межведомственных комиссий, исследующих тенденции развития современных информационно-коммуникационных технологий (ИКТ) и возникающие в связи с этим угрозы глобальной безопасности.

СОВРЕМЕННЫЙ КИТАЙ В КИБЕРПРОСТРАНСТВЕ: ДИНАМИКА РАЗВИТИЯ И ОСНОВЫ СТРАТЕГИИ

В отчетах и докладах органов различных государств Китай, как правило, с большим отрывом занимает первое место в списке стран, осуществляющих хакерские атаки и акты кибершпионажа. По оценке американских экспертов, в китайской армии существуют специальные подразделения, специализирующиеся на кибервойнах и способные при необходимости вывести из строя большинство объектов информационной инфраструктуры США[2]. Что характерно, Китай не склонен преувеличивать собственные достижения в киберпространстве. Китайские эксперты часто указывают на то, что безопасность информационных систем страны находится лишь на ранней стадии развития и весьма уязвима перед мерами и технологиями, прописанными в киберстратегиях ведущих мировых держав. Руководство Китая опасается в случае масштабной кибератаки потерять контроль над узловыми точками информационной инфраструктуры, чем могут воспользоваться для дискредитации страны внешние силы[3]. Эти опасения небеспочвенны. В *Индексе кибермогущества*, составленном *Economist Intelligence Unit* и консалтинговой компанией *Booz Allen Hamilton*, Китай занял лишь 13-е место[4], а в рейтинге стран с наиболее развитым сектором ИКТ — лишь 36-е[5].

Означает ли это, что данные западных спецслужб о кибермощи Поднебесной противоречат представлениям составителей рейтингов и самих китайцев? Вовсе нет. Китай отдает себе отчет в том, что в случае прямого противостояния с США его армия и вооружения пока не в состоянии обеспечить адекватный ответ. Поэтому для достижения и сохранения паритета с Западом власти активно занимаются разработкой киберсредств, которые в случае нападения на Китай способны вывести из строя всю информационную инфраструктуру противника. Главная слабость КНР заключается в неспособности самостоятельно создавать новые технологии. ИКТ,

функционирующие в Китае, — это, как правило, искусно скопированные и доработанные технологии, ставящие страну на путь *догоняющей модернизации*, пока не способной генерировать собственные разработки[6]. Тем не менее в последнее время наблюдается резкое увеличение инвестиций в сферу кибербезопасности, а реализация собственных проектов в области ИКТ стала приоритетным направлением инновационного развития[7].

В государственной стратегической программе инновационного развития КНР закреплены важные положения о развитии киберпространства и обеспечения его безопасности. Информационная безопасность для Китая — это прежде всего безопасность его инноваций, и в этом важная особенность подхода страны к вопросам информационной и кибербезопасности. Китайская модель инновационного развития основывается на четком следовании национальным интересам, непрерывном расширении научной и технической базы страны, активном привлечении инвестиций в разработку НИОКР, постоянном совершенствовании законодательства в сфере защиты интеллектуальной собственности. В программе признается, что в производстве высокотехнологичных продуктов в области ИКТ Китай все еще зависим от западных технологий, которые при помощи встроенных шпионских программ могут нанести вред всей китайской информационной инфраструктуре, инновационным разработкам и создать угрозу национальной безопасности страны. Снижение зависимости от западных ИКТ рассматривается как одно из важных средств обеспечения кибербезопасности КНР.

В Китае отсутствует единая стратегия развития киберпространства и обеспечения безопасности информационных систем, но это вовсе не означает, что отсутствует концептуальное обоснование значимости проблемы. Основным документом, в котором подчеркивается значимая роль ИКТ в жизни китайского общества, является Всеобъемлющая концепция национальной безопасности Китая[8]. В концепции отмечено, что информация в современном мире не только открывает много возможностей, но и создает угрозы политической, экономической, военной безопасности КНР. Большое внимание в документе уделено интернету как наиболее значимому, но наименее управляемому сегменту глобального информационного пространства.

ИНТЕРНЕТ В КНР: ИСТОРИЯ РАЗВИТИЯ И ИСТОКИ СТРАТЕГИИ РЕГУЛИРОВАНИЯ

Интернет в Китае впервые был запущен 20 сентября 1987 г. Тогда в Пекинском институте физики и высоких энергий профессор Цянь Тяньбай в рамках проекта CANET (Chinese Academic Network) отправил первое электронное письмо из Китая. Сайт института (http://www.ihep.ac.cn) — один из самых старых и наиболее известных в Китае и за рубежом — стал стартовой площадкой для многих государственных и коммерческих веб-страниц[9]. Содействие развитию китайского сегмента интернета оказали учебные заведения Германии и Канады. В октябре 1990 г. была зарегистрирована китайская доменная зона .cn, и в том же году официально открылся сервис электронной почты из этой доменной зоны[10]. В 1994 г. был осуществлен первый выход в интернет через 64 бит/с линию *Sprint*, и Китай международным сообществом был официально признан страной, обладающей полным набором функций интернета. Стремительному развитию интернета в Китае способствовал взятый компартией в 1995–1996 гг. курс на развитие китайской науки и техники, который включал и разработки в области интернета.

В настоящее время интернет в Китае пользуется большой популярностью: в конце декабря 2011 г. количество интернет-пользователей в стране составило 513 млн человек. Количество пользователей, использующих широкополосный доступ в интернет, составляет 93,5 млн человек[11]. Зона .cn стала рекордсменом по количеству зарегистрированных в ней доменов. При этом общее количество вебсайтов, зарегистрированных в доменной зоне .cn, в середине 2012 г. составляло более 2,3 млн[12].

Стремительное развитие и растущая популярность интернета в Китае поставили перед руководством компартии в 1990-е гг. двойственную задачу. С одной стороны, власти страны не хотели упускать из-под контроля ситуацию в стране, с другой — перед ней остро стояли задачи экономической модернизации, внедрения передовых технологий, ослабления остроты социальных проблем. Внутри политической элиты страны созрело понимание того, что решение этих проблем во многом зависит от уровня проникновения ИКТ во все сферы общественной жизни. Интерактивные технологии — действенный инструмент, способный максимально облегчить работу социальных и государственных институтов и создать своеобразную, доселе не виданную систему виртуальной демократии в стране с огромным и разнородным населением.

Но интернет весьма чувствителен к внешним влияниям технологий. Его свободное функционирование в Китае означало бы проникновение идей, нацеленных на дискредитацию политического строя государства. События на площади Тяньаньмэнь в 1989 г. сделали руководство страны весьма чувствительным к современным технологиям. Тогда посредством информационных ресурсов, в частности средств массовой информации, Западу удалось сформировать образ КНР как автократии, где права человека жестко ограничиваются. По этим причинам правительство Китая долго не могло определиться с тем, какую позицию занять по отношению к интернету. Но в 1996 г. государство дало добро на развитие глобальной сети в стране, и интерактивные технологии были включены в официальные планы развития китайской науки и техники[13].

Стратегия Китая по внедрению и развитию интернет-технологий отличалась от западного подхода. «Интернет — это орудие работы, а не средство времяпрепровождения», — этот лозунг, широко распространенный в стране, четко отражает отношение властей к новым средствам массовой коммуникации[14]. Овладение китайцами приемами работы в сети, а также получение информации, полезной для нации, по мнению властей, способны создать новые рабочие места, повысить жизненный уровень населения, ускорить развитие отсталых регионов, сформировать новую прогрессивную китайскую нацию, а значит, сделать Китай самодостаточной державой и помочь ей занять лидирующие позиции в мире во всех сферах жизнедеятельности.

Интернет-стратегия Китая на первом этапе основывалась на заимствовании технологических достижений развитых стран и адаптации их к специфике собственного экономического, политического, социального и культурного развития. На втором этапе китайское руководство приступило к созданию высокотехнологичных индустриальных зон и технопарков, где развивались интернет-технологии и воспитывались технические кадры.

В ноябре 2005 г. в Китае принята Государственная стратегия развития информатизации на 2006–2020 гг. В ней были сформулированы основные направления развития интернета. Важной задачей стало продвижение интернета в народном хозяйстве для корректировки экономической структуры, а также трансформация метода экономического роста и продвижение информатизации для строительства гармоничного общества[15]. Однако в числе первых задач, которые призван решить интернет, стоят повышение качества медицины и доступ широких масс китайцев к образованию. Эти два направления избраны не случайно. Дистанционная медицина позволяет диагностировать заболевания граждан, находящихся в отдаленных регионах и лишенных возможности приехать в центр на обследование[16]. Дистанционное образование оказалось серьезным подспорьем в решении задачи обеспечения всего населения средним образованием. Приоритеты в сфере сетевых услуг отдаются также банковской сфере, электронной коммерции. Правительство поощряет использование интернета для проведения научных исследований и развития бизнеса. Важным направлением политики Китая является внедрение *электронного правительства*.

Для обеспечения широкого доступа граждан к *онлайн*-услугам необходимо было внедрить интернет не только в крупных городах, но и в отдаленных населенных

пунктах. Началась кампания по повсеместному подключению поселков и деревень к интернету. В 2009 г. около 95% городов и поселков имели высокоскоростной доступ к глобальной сети, а жители 92,5% китайских деревень — возможность подключиться к интернету через телефонную линию[17].

Под воздействием государства быстро увеличивается число провайдеров интернет-услуг. Коммерческим провайдерам официально было разрешено заниматься предоставлением интернет-услуг в 1995 г. В настоящее время самыми крупными компаниями, предоставляющими услуги интернета, являются *China Telecom*[18], *China Mobile*[19] и *China Unicom*[20]. Основная инфраструктура китайского сегмента интернета состоит из девяти интернет-провайдеров, в ведении которых находятся все физические каналы, связывающие Китай с окружающим миром.

Китайский сегмент интернета разделен на несколько специализированных сетей, в которые входят:

- научно-исследовательская *China Science and Technology Network* (CSTNet, http://www.cnc.ac.cn); данная сеть объединяет НИИ, государственные научно-технические органы и некоторые академические учреждения;
- образовательная сеть *China Education and Research Network* (CERNET, http://www.edu.cn), объединяющая образовательные учреждения Китая, включая средние школы и университеты в крупных городах страны;
- коммерческие сети; наиболее крупные — *China Net* (http://www.bta.net.cn), государственная сеть, которая охватывает более 50% рынка интернет-услуг в стране и предоставляет интернет-сервис государственным организациям[21], а также *Golden Bridge Network* (GBNet, http://www.gb.co.cn).

Подобная *специализация* китайского интернета облегчает работу пользователям в сети и позволяет быстро ориентироваться во Всемирной Паутине в зависимости от целей и интересов, в то же время сегментация интернета позволяет властям контролировать деятельность *юзеров* и отслеживать все противоправные действия.

Массовое распространение интернета в Китае вовсе не означает, что компартия ослабила над ним контроль. Наоборот, борьба за предотвращение негативных для властей последствий от информации, распространяемой в Сети, лишь усилилась. Прилагаются огромные усилия для эффективной сетевой цензуры. В основном же наблюдение за работой пользователей ведется на местах и начинается уже с момента регистрации пользователя. Для того чтобы стать интернет-пользователем, физическое лицо должно пройти проверку в местном полицейском отделении и предоставить провайдеру справку установленного образца. По некоторым неофициальным данным, кадровые работники Министерства общественной безопасности нередко работают на руководящих должностях в крупных провайдерских фирмах.

Осознавая, что проконтролировать все действия китайских пользователей в сети невозможно, власти перераспределили функции контроля над Сетью между операторами связи и органами власти на местах. Главным органом, контролирующим интернет в Китае, является Министерство промышленности и информатизации. Министерство было создано в 2008 г. для развития в стране интернета, беспроводной связи, производства электронных и информационных товаров, индустрии программного обеспечения. При этом данное министерство несет ответственность лишь за обеспечение технического функционирования интернета и информационных технологий.

Регулирование контента и электронной медиаиндустрии возложено на другое ведомство — Государственное управление по делам радиовещания, кинематографии и телевидения. Оно ответственно за блокирование интернет-провайдерами на централизованном уровне доступа к порнографическим ресурсам и сайтам,

предлагающим азартные игры. Специальные фильтры, которые провайдеры интернета обязаны устанавливать за свой счет, блокируют также доступ к зарубежным ресурсам политического содержания, используя ключевые слова «диссидент», «Тайвань», «Тибет» и др. Они автоматически заменяются на точки, а сами сообщения удаляются. В число ресурсов, подвергающихся цензуре, входит большинство западных СМИ, сайты множества американских университетов, поисковая система *Alta Vista*. Нарушение данных правил влечет серьезное наказание: у провайдеров могут отобрать лицензию на предоставление услуг связи, а частным лицам грозит смертная казнь за публикацию материалов, не угодных правительству.

Китайские законы и нормативные акты, регулирующие развитие интернета, отличаются особой жесткостью. В 1994 г. Госсовет КНР издал Правила регулирования, обеспечивающие безопасность компьютерных и информационных систем, которые дали Министерству государственной безопасности права и полномочия на управление Сетью. В соответствии с правилами правительство имеет право нейтрализовать практически любой неугодный ресурс. К примеру, ответственность предусмотрена за публикацию «материалов, вредящих репутации государства», но интернет-пользователь не имеет никаких способов определения, вреден ли материал или нет (в сводах законов данное понятие никак не расшифровывается).

В соответствии с национальным законодательством, в Китае существует двухступенчатый доступ к интернету. На первом уровне пользователи могут выйти в мировую сеть лишь через магистральные узлы [backbone networks][22]. Существует ограниченное количество подобных ключевых узлов, которые находятся в ведении центральных министерств или групп, имеющих мощную политическую поддержку власти. На китайский интернет-трафик была наложена сложная система файрволов [system of firewalls][23], которая ограничивает доступ к *проблемным*, по мнению государства, внешним ресурсам. В стране успешно реализуется проект *Золотой щит* (неофициальное название — *Великий китайский файрвол*, игра слов по ассоциации с Великой китайской стеной), в рамках которого создана сложная система фильтрации содержимого интернета в КНР. В рамках проекта функционирует система серверов на интернет-канале между провайдерами и международными сетями передачи информации, которая фильтрует информацию. Файрволы применяются китайскими провайдерами для защиты от вирусов и хакеров, а также для блокирования доступа к определенным сайтам.

Китайское государство бдительно следит за тем, чтобы его граждане жили в соответствии с нормами, призванными обеспечить успешное построение коммунизма. Эти нормы подразумевают, что к гражданам не должна попадать *лишняя* информация. Если вебсайт содержит такую информацию, он фильтруется, и доступ к нему из Китая закрывают. Это относится не только к *антикоммунистическим* сайтам (а это большинство мировых ресурсов, например, интернет-энциклопедия *Wikipedia*). Китайские власти применяют репрессивные меры против антиправительственных акций внутри сети. Пересылка секретных или же реакционных материалов по IP-сетям считается государственным преступлением. Наказания для тех, кто нарушает правила пользования интернетом, варьируются от денежных штрафов до лишения права пользования интернетом.

В 2001 г. было организовано Китайское общество пользователей интернета, призванное служить развитию интернета, а по сути реализовывать решения правительства в сфере контроля над глобальной сетью. За годы существования общество разработало и приняло немало документов, регулирующих деятельность интернет-пользователей. Среди них Конвенция об отраслевой самодисциплине в сфере интернета КНР, Правила самодисциплины о запрете на распространение в интернете развратной, порнографической и другой недолжной информации, Конвенция о бойкотировании вредоносных программ, Конвенция о самодисциплине в области обслуживания блогосферы, Конвенция о самодисциплине в области борьбы с сетевыми вирусами, Манифест об отраслевой самодисциплине

в области издательского права в интернете и ряд других документов, призванных стимулировать здоровое развитие интернета[24].

В 2005 г. были введены усиленные меры по регламентированию деятельности граждан в интернете. Так, было запрещено анонимное общение, введена обязательная регистрация сайтов, проведена серия облав на владельцев нелегальных интернет-кафе. С 2006 г. в Китае начало свою работу специальное полицейское ведомство для контроля за интернетом. *Интернет-полицейские* призваны следить за содержанием сайтов, *онлайн*-форумов и социальных сетей. На многих, прежде всего крупных китайских сайтах, чтобы завести свой блог или оставить сообщение на форуме, нужно пройти обязательную регистрацию, при которой необходимо указать свои настоящие личные данные, включая имя, адрес и идентификационный номер. Все эти данные через компьютерный банк данных проверяют на подлинность, и только после этого регистрация считается пройденной.

К корпоративным пользователям всемирной сети предъявляются более жесткие правила пользования интернетом. Любая компания, желающая подключится к интернету, в течение нескольких месяцев проходит тщательную проверку. Определенные послабления со стороны цензоров имеют лишь крупные компании, которым в силу их коммерческой деятельности необходим доступ к более широкому контенту. Действия всех корпоративных клиентов фиксируются, нарушители наказываются. На предприятиях ведется журнал, где аргументируется посещение каждого сомнительного сайта. Распространена практика использования публичной электронной почты, когда группе сотрудников компании присваивается один и тот же адрес, а переадресация корреспонденции производится через системного оператора или дежурного администратора локальной сети[25].

Создать собственный интернет-сайт юридическому лицу также непросто. Каждый онлайн-ресурс должен получить лицензию, выданную Министерством промышленности и информатизации. Для этого компании необходимо иметь солидный уставный капитал. С 2008 г., согласно новым правилам, подавать заявки на получение лицензий на радиовещание или потоковую трансляцию (видео) *онлайн* могут только компании, принадлежащие властям или контролируемые государством. В 2009 г. вступил в силу закон о том, что для регистрации доменных имен в зоне .cn необходимо подавать письменное заявление, в котором помимо всех личных данных надо указывать и номер лицензии предприятия на коммерческую деятельность.

ДРАКОН В СЕТИ: КИТАЙСКАЯ КИБЕРУГРОЗА

Методы контроля, существующие в Китае, вовсе не означают, что интернет в стране отстает от западных тенденций развития глобальной сети. Китайская система управления интернетом весьма гибкая и предусматривает различные послабления для определенных категорий пользователей: ученых, работников СМИ, бизнесменов, в том числе иностранных инвесторов. Китайский рынок интернет-услуг — один из самых быстрорастущих, что особо привлекает внимание инвесторов. Примечательно, что, несмотря на действующую цензуру контента и фильтрацию трафика, большинство китайцев используют интернет для поиска новостей, участия в социальных сетях и развлечений, растет популярность *онлайн*-покупок. На китайский рынок вышли многие западные высокотехнологичные компании. Это обусловлено весьма благоприятными условиями, которые создают власти Китая. Поощряются научные и прикладные исследования зарубежных компаний в КНР, внедряется система так называемых *информационных портов* — зон свободного таможенного и налогового регулирования, ориентированных на развитие инновационных технологий, электронной коммерции и информатики.

Активное привлечение западных технологий и иностранных инвестиций вовсе не означает, что они свободно ведут свою деятельность в стране и неподконтрольны власти. Госсовет КНР рассматривает интернет как важный объект государственной инфраструктуры, который должен находиться в рамках суверенного

управления Китая. Посягательства на китайский сегмент интернета со стороны внешних сил рассматриваются как угроза национальной безопасности. Иностранные граждане и компании, находящиеся в КНР, при пользовании глобальной сетью должны следовать нормам законодательства и требованиям властей. Любое иностранное юридическое лицо, перед тем как войти на китайский рынок, принимает правила игры китайского правительства и вынуждено действовать в соответствии с ними[26]. Так, компания, специализирующаяся на предоставлении услуг в сфере ИКТ, прежде, чем выйти на рынок, обязана получить лицензию на свою деятельность в Министерстве промышленности и информатизации, так же как и любая китайская компания. Именно из-за отсутствия такой лицензии у китайского подразделения компании *Google* в самом начале работы возникли проблемы.

Еще одно требование Госсовета КНР к иностранным компаниям — это фильтрация трафика и недопущение распространения информации, способной дискредитировать власть. В данной связи показателен инцидент с *Google*, когда весной 2010 г., невзирая на многочисленные предупреждения госструктур, интернет-поисковик отказался фильтровать в сети запросы китайских пользователей. В ответ Китай обвинил *Google* в нарушении *письменного обещания* о подчинении китайским законам, сделанного компанией при выходе на китайский рынок. В ответ компания заявила, что перенаправит китайских пользователей на нецензурируемые страницы своего гонконгского сайта. В защиту поисковика выступил представители Белого дома США, выразив обеспокоенность невозможностью разрешить конфликт и нарушением свободы слова в Китае. Это обострило и без того непростые отношения США и КНР[27]. Политическая подоплека произошедшего скандала позволила обрести мощные рычаги сдерживания китайской экспансии, в частности экспорта ИКТ на мировые рынки, за счет обвинений в отсутствии демократии и свободы слова в Китае, а корпорация *Google* приобрела отличный административный ресурс в Вашингтоне.

Открытость Китая для привлечения передовых западных ИКТ, тем не менее, носит односторонний характер и проявляется главным образом в восприимчивости к передовому зарубежному опыту в этих областях. Собственные разработки широко не афишируются, а между тем благодаря своей относительной дешевизне они активно завоевывают мировой рынок. Продукция, произведенная в Китае, уже давно не вызывает того пренебрежения и недоверия, которые импортеры и рядовые покупатели испытывали еще несколько лет назад при виде надписи *Made in China*. Ныне огромный ассортимент инновационной продукции, начиная от ноутбуков, мобильных коммуникаторов, *iPhone*, GPS-навигаторов, не уступает европейским, американским и японским аналогам. Например, китайская компания *Huawei Technologies* — одна из крупнейших в стране, специализирующаяся в сфере телекоммуникаций. Компания занимает ведущие позиции в мире по изготовлению ноутбуков, оборудования беспроводных сетей, программного обеспечения. Продукцию компании используют 35 из 50 крупнейших мировых операторов связи. Американские военные аналитики причисляют *Huawei Technologies* к главной угрозе безопасности США не только в информационной, но и в военной сфере. Это обусловлено тем, что компания поддерживает тесные связи с китайскими военными. В частности, основатель и бессменный глава *Huawei Technologies* Жень Чженфей в молодые годы служил в Народно-освободительной армии Китая (НОАК). На основе этого и многих других подобных фактов делаются выводы о том, что в производимых компанией *Huawei* технологиях, поставляемых в том числе в США, встроены аппаратные закладки и другие вредоносные шпионские программы[28].

Распространение вредоносных программ — не единственное зло, которое приписывают Китаю в киберпространстве. В отчетах западных разведслужб КНР называют одной их основных стран, откуда исходят угрозы информационной безопасности. Китаю не удается, как прежде, показывать свое невежество и невиновность при проведении кибератак и разведки в киберпространстве США. По данным компании *Northrop Grumman*[29], которая занималась подготовкой отчета для американо-китайской комиссии по отношениям в области экономики и безопас-

ности[30] *«Занимая информационную высоту: возможности Китая по проведению компьютерных сетевых операций и кибершпионажу»,* в китайской армии уже есть подразделения, специализирующиеся на ведении операций в киберпространстве. Существование подразделения кибервойск, которое носит название *Голубая кибермия*, открыто признал министр обороны Китая Генг Яншенг[31]. По оценке американских экспертов, их общая численность может составлять 30 тыс. военнослужащих. В докладе отмечается, что за последние 10 лет было зафиксировано множество случаев проникновения в информационные системы США, в результате которых Китай овладел коммерческими и военными данными. Обширные возможности КНР в области кибершпионажа объясняются активной разработкой киберсредств, которые финансируются со стороны правительства[32].

Эффективность китайских киберподразделений обусловлена тесным сотрудничеством между правительственными структурами, военными и хакерами. Китайские военные видят успех современных боевых действий в способности контролировать информацию и информационные системы противника. Руководство Народно-освободительной армии Китая (НОАК) рассматривает компьютерные сетевые операции как важный элемент информационного противоборства, и стремится объединить все элементы информационной войны (электронные и неэлектронные, наступательные и оборонительные) в единую систему[33]. В отчете компании *Northrop Grumman* отражены конкретные доктринальные намерения, а также сведения о финансовой поддержке Китаем систематического кибершпионажа. Основные положения стратегии информационной войны отражены в Военно-политическом руководстве Китая. Они были внесены в документ в 2002 г., когда НОАК объявило о возрастающей необходимости противостоять врагам в условиях высокотехнологичных войн. Тогда же были сформулированы основные направления оборонной политики КНР, где особый акцент сделан на модернизацию вооруженных сил за счет их информатизации. В документе впервые появилась формулировка «противостояние в локальных войнах в условиях информатизации вооруженных сил», обусловливающая необходимость преобразования вооруженных сил Китая[34].

В рамках НОАК существует детально разработанная доктрина о нападении на компьютерную инфраструктуру противника. Пекин делает ставку именно на этот вид оружия, поскольку по остальным компонентам настолько уступает США, что не надеется сократить разрыв в ближайшие годы. НОАК вербует в свои подразделения некоторых хакеров, а также может использовать их для проникновения в иностранные компьютерные сети. Вывод из строя сетевой инфраструктуры противника, рассчитывают в НОАК, может *ослепить* и задержать мощнейшую в мире американскую армию, что позволит Китаю выиграть время и предотвратить одномоментный полномасштабный удар[35].

Примером проникновения китайских хакеров в американскую информационную инфраструктуру является беспрецедентное по масштабам отключение электроэнергии на северо-западе США в 2003 г. В результате выхода из строя энергосети пострадали около 50 млн человек в штатах Огайо, Нью-Йорк, Мичиган, а также в некоторых штатах Канады. По данным американских спецслужб, за этим отключением стоял Пекин, испытывавший возможности своих киберподразделений. Еще один громкий скандал разгорелся после взлома китайскими хакерами учетных записей нескольких сотен пользователей почтового сервиса *Gmail* компании *Google*, в том числе аккаунтов высокопоставленных американских чиновников. Взлом начался с сообщения, отправленного сотруднику *Google* через программу *Microsoft Messenger*. Нажав на ссылку, сотрудник зашел на зараженный сайт и невольно предоставил злоумышленникам доступ к своему компьютеру, а затем и к компьютерам разработчиков в штаб-квартире компании. Хакерам удалось получить контроль над хранилищем разработок соответствующего отдела[36].

Для расширения возможностей Китая в киберпространстве НОАК активно взаимодействует с коммерческими организациями и сферой образования, что способствует получению доступа к передовым исследованиям и технологиям, в том числе к телекоммуникационным системам военного и двойного назначения. В 50 китай-

ских университетах национальное правительство финансирует различного рода программы, направленные на поддержание исследований в области организации и проведения кибератак и кибероборонь, в том числе связанных с проведением информационной войны. Зачастую эта работа осуществляется посредством взаимодействия с зарубежными партнерами, проводящими исследования в сфере критических технологий[37].

Впрочем, китайские хакеры зачастую организуют атаки на киберпространство иностранных государств самостоятельно и без ведома чиновников. Первой организованной группой китайских хакеров считается группировка *Зеленый отряд*. Она была основана в 1997 г. и существовала как форум для любителей сетевых технологий, которые обменивались опытом по взлому различных систем сетевой защиты. Хакеры из этой группы сыграли ключевую роль в организации кибервойны против Индонезии в 1997 г. Причиной кибератак стали антикитайские погромы в Индонезии в 1998 г., возникшие после финансово-экономического кризиса. Предпосылкой вспыхнувших волнений стал тот факт, что проживающие в Индонезии выходцы из Китая практически полностью взяли под свой контроль послекризисное распределение продовольствия на большей части территории страны[38]. Суть организованной *Зеленым отрядом* кибервойны заключалась в том, что хакеры группировки вывешивали инструкции о том, как атаковать индонезийские правительственные сайты, засылая на их серверы многочисленные электронные письма. Более продвинутые члены группы взламывали сайты и размещали на них записи, призывающие остановить атаки на *хуацяо* — выходцев из Китая. Пик кибератак пришелся на национальный праздник Индонезии — 17 августа, День независимости. Джакарта тогда обвинила официальный Пекин в организации кибервойны.

Китайские хакеры называют себя *хункэ* (*красный гость*) по аналогии с китайским словом *хакер — хэйкэ* (*черный гость*). В 1999 г., после того как американская авиация по ошибке разбомбила посольство КНР в Белграде, они организовали атаки на американские правительственные сайты, в результате которых был впервые взломан сайт Белого дома. Аналогичные действия были предприняты и в мае 2001 г., когда над островом Хайнань столкнулись китайский истребитель и американский самолет-разведчик. По подсчетам самих китайцев, тогда было взломано 1036 американских сайтов, включая 18 военных и 39 правительственных[39].

Китай весьма критично относится к существующему международному режиму управления интернетом, где основные функции по присвоению имен и адресов интернета закреплены за подотчетной США Корпорации по распределению имен и адресов (ICANN). На различных международных форумах, где обсуждаются вопросы управления интернетом, представители Китая всегда жестко критикуют деятельность ICANN, обвиняя ее в пособничестве американцам. Неприятие Китаем деятельности ICANN особенно усилилось после выдачи корпорацией домена .tw Тайваню, официально рассматриваемому Китаем в качестве провинции в составе национальной территории[40]. Главное требование КНР заключается в роспуске корпорации и создании подлинно международной организации, управляющей интернетом под эгидой ООН. В сентябре 2011 г. Китай, Россия и другие страны представили Генеральной Ассамблее ООН проект Правил поведения в области обеспечения международной информационной безопасности и призвали к тому, чтобы страны в рамках ООН провели обсуждение по этому документу и достигли договоренности в международных правилах и нормах всех стран по действиям в информационном пространстве. Предложенный документ призывает к упорядочиванию международных правил в сфере сетевой безопасности и в корне отличается от инициатив в области информационной безопасности, выдвигаемых США и Евросоюзом, где в случаях, угрожающих национальной безопасности, допускается проникновение госструктур в международные информационные сети.

Шанхайская организация сотрудничества (ШОС) — еще одна площадка, которую Китай стремится использовать для регулирования интернета и обеспечения безопасности информационных систем. В частности, вопросы информационной безопасности нашли отражение в заявлении глав государств — членов ШОС

по международной информационной безопасности от 2006 г. на саммите в Шанхае, Екатеринбургской декларации ШОС от 2009 г.[41] и Ташкентской декларации ШОС от 2010 г. В перечисленных документах информационная безопасность рассматривается как важный фактор обеспечения государственного суверенитета, национальной безопасности, социально-экономической стабильности[42].

Однако в вопросе управления интернетом Китай зачастую не ограничивается лишь декларативными документами и намерениями, а переходит к конкретным предложениям и действиям. В частности, Китай предлагает увеличить контроль государств над архитектурой глобального управления интернетом с помощью создания альтернативной версии системы доменных имен — DNS-расширения для автономного интернета[43]. Основные цели внедрения системы альтернативных доменов — снижение зависимости от глобального интернета и создание *автономного интернета*, функционирующего в рамках одного государства. Это позволит пользователям снизить зависимость от иностранных доменов, таких как .com, .net и других, а правительству Китая обойти ICANN и искоренить официальную систему доменных имен в пользу национальных систем. Чтобы не нанести вред существующей системе доменных имен, прежде чем будет создано множество AIP-сетей, каждая страна может независимо от других создать AIP-сеть и подключиться к интернету по исходной ссылке, считают китайские власти. Предполагается, что при таком подходе возможно будет также объединять сети двух и более государств, создавая единую AIP-сеть. Это позволит улучшить *масштабируемость* интернета. Помимо этого, определенные страны смогут ввести лучший контроль над местными сегментами интернета. Китай неоднократно озвучивал эту инициативу на международных форумах по управлению интернетом, а в июне 2012 г. официально подал заявку в Инженерный совет интернета на введение нового стандарта на «расширение DNS для автономного интернета»[44].

КИТАЙСКАЯ ГОСУДАРСТВЕННАЯ ПРОПАГАНДА И СОЦИАЛЬНЫЕ СЕТЕВЫЕ СЕРВИСЫ

Китайские власти видят в интернете и современных ИКТ не только средство устрашения противников, но и большие возможности для формирования позитивного имиджа страны на международной арене. В стране создано специальное Административное бюро по пропаганде в интернете, созданное при Информационном агентстве Государственного совета КНР. Оно направляет и координирует государственную пропаганду в Сети. Еще несколько лет назад основными проблемами развития интернета в Китае были недостаток сайтов, созданных непосредственно в Китае, и дефицит контента на китайском языке. Большинство существовавших в стране печатных и электронных СМИ не имели собственных сайтов в интернете и не были представлены широкой аудитории. Ситуация начала меняться в начале прошлого десятилетия, когда Госсовет КНР осознал, что интернет — это удобный механизм реализации определенных политических и социальных программ. Началось широкое инвестирование не только в масс-медиа на китайском языке, но и в расширение китайских иноязычных СМИ.

На первом этапе власти стимулировали создание интернет-сайтов наиболее крупных информационных агентств, расширили сетку их вещания и распространения. На втором этапе было увеличено количество зарубежных корпунктов государственного информационного агентства *Синьхуа* до 186 и расширена сфера его деятельности на спутниковое и интернет-телевидение. Не менее важной задачей стал запуск китайских СМИ в интернете на иностранных языках, что позволило жителям различных стран и континентов получать информацию из Китая *из первых рук*. Центральное телевидение Китая *CCTV* запустило вещание на английском, французском, испанском, русском, арабском языках, наняв для этих целей более 100 новых иностранных сотрудников.

В 2009 г. медиахолдинг *Жэньминь Жибао* выпустил англоязычную версию газеты по международной проблематике *Хуаньцю Шибао*, которая стала вторым в Китае

Нандан ***Унникришнан****, директор по евразийским исследованиям, старший научный сотрудник Исследовательского фонда Observer, Рахул* ***Пракаш****, младший научный сотрудник, Институт исследований безопасности, Исследовательского фонда Observer — по электронной почте из Дели:* В киберпространстве эффективная оборона невозможна без создания потенциала нападения. К примеру, для того чтобы пресечь кибератаку, государству может быть необходимо вывести из строя компьютерные сети за пределами его национальной территории. Например, Индии на случай конфликта с Китаем необходимо заранее готовиться к возможной кибератаке, нацеленной на выведение строя сетей системы военного командования и управления. Обеспечение информационного превосходства за счет вывода из строя сетевых систем противника, отвечающих за управление, связь, сбор и передачу данных, наблюдение и разведку местности, является центральным элементом китайской стратегии кибервойны, которая органично вписывается в общую военную стратегию КНР. Другим вероятным противником в киберпространстве для Индии является Пакистан, с территории которого ранее осуществлялись кибератаки, нацеленные в числе прочих на индийские органы безопасности. Можно ожидать, что индийские военные готовятся к отражению подобных угроз китайского или пакистанского происхождения.

ежедневным изданием на английском языке после *China Daily.* Данные издания начали активно представлять себя, в том числе в интернете, что резко увеличило аудиторию их читателей по всему миру. Важным этапом в *завоевании* глобального информационного пространства стала практика приобретения долей в иностранных СМИ. Так, в июле 2009 г. владелец пекинской медиакомпании *Xiking Group* заявил о намерении приобрести британский телеканал *Propeller TV* и создать на его основе двуязычный англо-китайский проект, ориентированный на освещение Китая и пропаганду китайской культуры. Увеличение китайских масс-медиа в интернете, рассчитанных на зарубежную аудиторию, создает возможности для властей Китая усилить пропаганду на зарубежные государства и создать иллюзию многообразия источников информации и плюрализма мнений в Китае[45]. Данные тенденции объективно способствуют усилению позиций КНР в глобальном информационном пространстве.

Вместе с тем китайцы начали активно использовать интернет для противодействия критике, звучащей в адрес Китая извне. После событий в 2008 г. в Тибете и в Синьцзян-Уйгурском автономном районе (СУАР) в 2009 г. в западных СМИ было опубликовано множество негативных и не всегда полностью достоверных материалов о действиях китайских властей. Китайские пользователи стали размещать на популярных в стране интернет-порталах *Sina.com* и *China.com* ссылки на конкретные искажения с требованиями опровержения. Был даже создан специальный сайт *Anti-CNN.com*. В результате активной позиции китайских блогеров удалось добиться извинений от некоторых западных СМИ. Таким образом, в современной китайской внешнеполитической пропаганде проявляется стремление Пекина перехватить инициативу, действовать не в ответ на иностранные выпады, а на упреждение, порой даже в наступательном ключе[46].

Большой популярностью в Китае пользуются ведение блогов и участие в социальных сетях. При этом большая часть блогов пишется именно на китайском языке. *Facebook*, *Twitter*, *Livejournal* и другие иностранные социальные веб-сервисы блокируются в стране, поэтому основным ресурсом, на котором ведутся блоги, явля-

ется *Sina Weibo*, который занимает третье место по популярности в Китае. В китайской сегменте интернета существует свыше миллиона форумов, зарегистрировано 220 млн блогеров. Каждый день посредством социальных сетей, блогов, форумов публикуется свыше трех миллионов записей, более 66% китайских пользователей интернета часто выкладывают в сети свои записи, комментируют, жалуются или выражают свою точку зрения на разные темы. Новые функции и новые услуги, предлагаемые интернетом, предоставили более широкое пространство для выражения людьми своих взглядов[47]. Вторым по популярности социальным ресурсом в КНР является социальный портал *51.com*. На нем зарегистрировано 120 млн пользователей. Ежедневно на сайте регистрируются 100 тыс. новых пользователей. Это привлекает инвесторов во всем мире. *Zhanzuo.com*, на котором зарегистрировано семь миллионов пользователей, — еще одна популярная социальная сеть в Китае. Этот ресурс в 2007 г. планировал купить владелец *Facebook* Марк Цукерберг за 85 млн долл., однако стороны так и не пришли к компромиссу, и сделка сорвалась.

В отношении социальных сетей и блогов власти Китая проводят ту же политику тотального контроля, что и в отношении других интернет-ресурсов. Блогхостингам запрещено предоставлять услуги пользователям, не оставившим при регистрации свои подлинные и полные данные. Регистрация пользователей под псевдонимами запрещена. Причем авторизованы в блогосфере Китая должны быть и комментарии — анонимные мнения также вне закона. Для усиления контроля над социальными сетями интернет-сервис *Sina Weibo* ввел в действие новые правила для предотвращения распространения в сети слухов и призывов к акциям протеста. Все 324 млн человек, зарегистрированных в этой социальной сети, получили на свой счет 80 баллов, которые будут отниматься за нарушения правил. Штрафы планируется налагать «за призывы к нелегальной деятельности, нарушению порядка путем создания незаконных организаций», а также «к организации неразрешенных протестов, демонстраций и собраний». Блогеры понесут наказание и за распространение слухов, «затрагивающих честь Китая и подрывающих стабильность в обществе». При исчерпании лимита в 80 баллов аккаунты пользователей будут удаляться[48].

Несмотря на существующие меры контроля социальных ресурсов, китайские пользователи находят способы, чтобы обойти их. Так, для входа *Facebook* и *Twitter* широко используются прокси-серверы и другие ресурсы, позволяющие обходить цензуру. Для обсуждения социально-политических вопросов используются слова, на первый взгляд не имеющие отношение к политике. Например, опальному политику Бо Силаю присвоили имя *помидор*. Его арестовали и отстранили от должности в марте 2012 г. по подозрению в коррупции. Его главный противник, премьер-министр Вэнь Цзябао, получил в блогах кличку *телепузик*. Вместо имени китайского художника-диссидента Ай Вэйвэя в интернете употребляют схожий по написанию иероглиф *любовь к будущему*, а историю слепого адвоката Чэнь Гуанчэна, сбежавшего из-под домашнего ареста и получившего убежище в США, блогеры обсуждали при помощи иероглифа *Шоушенк* (отсыл к голливудскому фильму «Побег из Шоушенка»). Так, при помощи использования каламбуров, омонимов, аббревиатур китайских названий на английском языке блогеры обсуждают важные политические процессы, стараясь не привлекать внимание цензоров. Поскольку эти методы общеизвестны, то и цензура их учитывает, часть из закодированных сообщений уже удалены из сети[49], но удалить все комментарии цензура не в состоянии. В условиях, когда социальные ресурсы стремительно развиваются, властям вряд ли удастся заделать все трещины в великой китайской *интернет-стене*.

ЗАКЛЮЧЕНИЕ

На основе анализа тенденций развития интернета в Китае и методов, используемых для обеспечения информационной безопасности, можно сделать вывод о том, что глобальная сеть в Поднебесной рассматривается как специфическая

инновационная среда, в рамках которой происходит формирование нового Китая и врастание его в мир. Для этого страна стремится максимально полно использовать экономические и пропагандистские возможности интернета и других интерактивных технологий.

Главным сторонником и двигателем китайского интернета является государство, и только оно определяет, какие опасности и возможности может таить в себе тотальная информатизация страны с населением, численность которого превышает 1 млрд человек. Властям крайне выгодно появление относительно дешевого средства массовой информации, достаточно мощного с точки зрения возможности воздействия на зарубежную аудиторию и в то же время вполне *управляемого*, чтобы ограничить обратное воздействие.

Отличительной чертой китайского интернета является четкая регламентация не только технических и организационных процедур, но и поведения пользователей в виртуальном пространстве. О свободе слова в Китае не принято говорить вообще, а интернет здесь является свободной зоной лишь теоретически. В действительности же пользователи имеют целый ряд обязанностей и вынуждены считаться с ограничениями, накладываемыми на использование сети контролирующими органами.

В интересах достижения лидирующих позиций на мировой арене Китай активно занимается разработкой киберсредств. Руководству КНР становится все сложнее показывать свое невежество и невиновность при проведении активной разведки радиоэлектронных средств и проникновении в киберпространство зарубежных государств. Эффективность китайских кибератак объясняется тесным сотрудничеством между правительственными структурами и хакерами.

Для расширения возможностей Китая в киберпространстве НОАК активно взаимодействует с коммерческими организациями и сферой образования, что способствует получению доступа к передовым исследованиям и технологиям, в том числе к телекоммуникационным системам военного и двойного назначения. Снижение зависимости от информационно-коммуникационных технологий Запада и развитие собственного инновационного потенциала рассматриваются как важные средства обеспечения кибербезопасности КНР.

Посредством широкого инвестирования в интернет-технологии, в частности нацеленного на стимулирование создания СМИ в интернете и развитие социальных сетей, Китай стремится сформировать позитивный имидж государства на международной арене и *смягчить* за счет создания эффекта *плюрализма мнений* негативное восприятие зарубежной аудиторией некоторых проблем внутриполитического развития страны. Вместе с тем, стремясь расширить информационные каналы, вещающие из Китая, власти страны стремятся контролировать воздействие зарубежных СМИ на китайскую аудиторию. Но в условиях, когда интернет-технологии продолжают активно развиваться и внедряются в жизнь китайского общества, властям становится все сложнее контролировать и фильтровать трафик и контент.

Примечания

[1] Сунь Цзы. Искусство войны. М.: София, 2010. С. 56–58.

[2] Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage. Prepared for the U.S.–China Economic and Security Review Commission by Northrop Grumman Corp. 2012, 7 марта,

http://http://www.uscc.gov/RFP/2012/USCC%20Report_Chinese_CapabilitiesforComputer_NetworkOperationsandCyberEspionage.pdf (последнее посещение — 30 августа 2012 г.).

[3] Segal A. Is China a Paper Tiger in Cyberspace? Council on Foreign Relations. 2012, 8 февраля, http://blogs.cfr.org/asia/2012/02/08/is-china-a-paper-tiger-in-cyberspace/(последнее посещение — 30 августа 2012 г.).

[4] Там же.

[5] Глобальный отчет по информационным технологиям 2010–2011 гг. Всемирный экономический форум. 2012, 13 января, http://strategy.ru/the-report-on-information-technology-2010–2011/(последнее посещение — 30 августа 2012 г.).

[6] Дынкин А., Пантин В. Мирное столкновение. *Россия в Глобальной Политике*. 2012. № 1 (март-апрель).

[7] По расходам на НИОКР страна уже вышла на второе место в мире после США.

[8] Гуанкай С. Всеобъемлющая концепция национальной безопасности Китая. *Россия в Глобальной Политике*. 2009. № 3 (май-июнь); Lu Yongxiang. Science &Technology in China: A Roadmap to 2050. Chinese Academy of Science, 2010.

[9] Мальцев А. Китайский Интернет: как за каменной стеной. *Вебпланета: журнал для подключенных.* 2009, 3 июня, http://http://www.webplanet.ru/review/life/2008/06/11/china.html (последнее посещение — 30 августа 2012 г.).

[10] Интернет в Китае. Справка. *РИА Новости*. 2010, 13 января, http://ria.ru/world/20100113/204310750.html (последнее посещение — 30 августа 2012 г.).

[11] Число пользователей интернета в Китае превысило размеры населения США. *РИА Новости*. 2009, 26 июля, http://ria.ru/society/20090726/178669834.html (последнее посещение — 30 августа 2012 г.).

[12] Число пользователей интернета в Китае превысило полмиллиарда человек, больше двух миллионов сайтов. *Gazeta.ru*. 2012, 17 января, http://http://www.gazeta.ru/news/lenta/2012/01/17/n_2168345.shtml (последнее посещение — 30 августа 2012 г.).

[13] Мажаров И. Интернет в Китае. *Мир Интернет.* 2008, 2 февраля, http://abirus.ru/content/564/581/582/591.html (последнее посещение — 30 августа 2012 г.).

[14] Ball D. China's Cyber Warfare Capabilities. *Security Challenges*. 2011. Vol. 7, No. 2 (Winter), http://www.securitychallenges.org.au/ArticlePages/vol7no2Ball.html (последнее посещение — 30 августа 2012 г.).

[15] Положение интернета в Китае. Пресс-канцелярия госсовета КНР. 2011, 1 февраля, http://russian.china.org.cn/government/archive/baipishu/txt/2011–02/01/content_21857458_8.htm (последнее посещение — 30 августа 2012 г.).

[16] Мажаров И. Цит. соч.

[17] Число пользователей интернета в Китае превысило размеры населения США. *РИА Новости*. 2009, 26 июля, http://ria.ru/society/20090726/178669834.html (последнее посещение — 30 августа 2012 г.).

[18] *China Telecom* — китайская государственная компания телекоммуникаций, создана в 2002 г. и занимается предоставлением комплексных информационных услуг, в частности фиксированной телефонной свяи, мобильной связи, подключением и использованием интернет-сети. Включена в рейтинг 500 самых крупных предприятий мира. Общий объем капитала компании составляет 632,2 млрд юаней, общий объем операционных доходов за весь год превысил 220 млрд юаней. В компании работают 670 тыс. сотрудников.

[19] *China Mobile* — китайская телекоммуникационная компания, создана в 1997 г. выделением из китайской государственной телекоммуникационной монополии *China Telecom*. Штабквартира компании расположена в Гонконге. Крупнейший в мире по количеству абонентов (493 млн по состоянию на 2009 г. и капитализации оператор сотовой связи. По состоянию на 2010 г. *China Mobile* контролировала около 70% китайского рынка.

[20] *China Unicom* — оператор связи в КНР. Компания основана в качестве государственной корпорации в 1994 г. Министерством промышленности и информационных технологий КНР. Предоставляет широкий выбор услуг, включая общенациональную сотовую GSM-сеть, международную и местную телефонную связь, обмен данными, услуги широкополосного доступа в интернет и IP-телефонии. На конец апреля 2008 г. компания имела 125 млн GSM-пользователей и 43 млн подписчиков. По состоянию на 2010 г. *China Unicom* контролировала около 20% китайского рынка.

[21] Ball D. China's Cyber Warfare Capabilities. *Security Challenges*. 2011. Vol. 7, No.2 (Winter), http://www.securitychallenges.org.au/ArticlePages/vol7no2Ball.html (последнее посещение — 30 августа 2012 г.).

[22] *Магистральные узлы* (*backbone networks*) — общий термин для обозначения совокупности базовых узлов распределенной сети, соединенных высокоскоростными магистральными каналами. Сегменты сети масштаба предприятия, а также кластеры и отдельные станции подключаются к магистральной сети через мосты, маршрутизаторы и концентраторы. Особые требования предъявляются к надежности магистральной сети. Традиционная магистральная сеть называется распределенной, что подчеркивает ее отличие от локализованной и коммутирующей магистралей.

[23] *Firewall* (*файрвол*, синоним — *брандмауэр*) — компьютер, маршрутизатор или другое коммуникационное устройство, ограничивающее доступ к защищаемой сети и осуществляющий контроль и фильтрацию перехватываемых сетевых пакетов в соответствии с заданными правилами.

[24] Положение интернета в Китае.

[25] Мажаров И. Цит. соч.

[26] Положение Интернета в Китае.

[27] Тодрес В. Китай после *Google* — конец миссионерского капитализма? *TV. Net.UA.* 2010, 21 января, http://http://www.gzt.ru/column/283744.html (последнее посещение — 30 августа 2012 г.).

[28] Бывший аналитик Пентагона заявил, что Китай может перекрыть весь механизм телекоммуникации на оборудовании, которое было продано им в США. *Военно-политическое обозрение.* 2012, 13 июня, http://http://www.belvpo.com/12173.html (последнее посещение — 30 августа 2012 г.).

[29] *Northrop Grumman* — одна из наиболее высокотехнологичных компаний ВПК США, занимающаяся разработками в области электроники и информационных технологий, авиакосмической отрасли, судостроения и др. Кроме того, корпорация занимается разработкой перспективного вооружения для министерства обороны США, а также проведением исследований, направленных на совершенствование средств и методов защиты информации.

[30] Комиссия по американо-китайским отношениям в области экономики и безопасности *(The U.S.–China Economic and Security Review Commission)* была создана Конгрессом США в 2000 г. и получила полномочия вести мониторинг и расследования различных аспектов торгово-экономических и военных взаимоотношений с Китаем. Организация регулярно представляет доклады Конгрессу США, а также имеет возможность вырабатывать рекомендации по изменению законодательных и административных мер, влияющих на отношения между двумя странами.

[31] В Китае появились *кибервойска*. *Chip.Ru*. 2011, 31 мая, http://http://www.ichip.ru/mobile/novosti/sobytiya/2011/05/v-kitae-poyavilis-kiber-voiska/mobile_view (последнее посещение — 30 августа 2012 г.).

[32] Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage. Prepared for the U.S.–China Economic and Security Review Commission by Northrop Grumman Corp. 2012, 7 марта,

http://http://www.uscc.gov/RFP/2012/USCC%20Report_Chinese_CapabilitiesforComputer_NetworkOperationsandCyberEspionage.pdf (последнее посещение — 30 августа 2012 г.).

[33] Юрченко Г. Возможности Китая по проведению компьютерных сетевых операций и кибершпионажу. *Военно-политическое обозрение*. 2012, 20 апреля, http://http://www.belvpo.com/9984.html (последнее посещение — 30 августа 2012 г.).

[34] Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage. Prepared for the U.S.–China Economic and Security Review Commission by Northrop Grumman Corp. 2012, 7 марта,

http://http://www.uscc.gov/RFP/2012/USCC%20Report_Chinese_CapabilitiesforComputer_NetworkOperationsandCyberEspionage.pdf (последнее посещение — 30 августа 2012 г.).

[35] Черненко Е., Габуев А. Оружие к сбою. *Коммерсантъ.* 2011, 15 февраля. № 26 (4567), http://http://www.kommersant.ru/doc/1585823 (последнее посещение — 30 августа 2012 г.).

[36] Markoff J. Cyberattack on Google Said to Hit Password System. *The New York Times*. 2010, 19 апреля, http://http://www.nytimes.com/2010/04/20/technology/20google.html?_r=2 (последнее посещение — 30 августа 2012 г.).

[37] Юрченко Г. Возможности Китая по проведению компьютерных сетевых операций и кибершпионажу. *Военно-политическое Обозрение*. 2012, 20 апреля, http://http://www.belvpo.com/9984.html (последнее посещение — 30 августа 2012 г.).

[38] Другов А. Политическая культура. Массовое насилие в Индонезии: социальные, культурные и политические корни. *East View*. 2000, 11 января, http://dlib.eastview.com/browse/doc/2450717?enc=rus (последнее посещение — 30 августа 2012 г.).

[39] Габуев А. Желтая киберугроза. Китай готовится к войнам в киберсети. *Коммерсантъ-Online*. 2011, 15 февраля, http://http://www.kommersant.ru/doc/1585979 (последнее посещение — 30 августа 2012 г.).

[40] Подробнее см. в настоящем номере *Индекса Безопасности*: Якушев М. Интернет–2012 и международная политика. *Индекс Безопасности*. 2013. Весна. №1 (104). С. 29–42.

[41] Екатеринбургская декларация глав государств — членов Шанхайской организации сотрудничества. Президент России. Официальный сайт. 2009, 16 июня, http://archive.kremlin.ru/text/docs/2009/06/217868.shtml (последнее посещение — 30 августа 2012 г.).

[42] Декларация 10-го заседания Совета глав государств — членов Шанхайской организации сотрудничества. Центральный портал Шанхайской организации сотрудничества. 2010, 12 июня, http://http://www.infoshos.ru/ru/?id=74 (последнее посещение — 30 августа 2012 г.).

[43] DNS-расширение для автономного Интернета (AIP) — способ работы альтернативных корневых DNS-серверов в пределах национальных границ при помощи особых шлюзов.

[44] Китай предложил «расширить DNS для автономного интернета». *SecurityLab*. 2012, 21 июня, http://http://www.securitylab.ru/news/426071.php (последнее посещение — 30 августа 2012 г.).

[45] Евдокимов Е. Политика Китая в глобальном информационном пространстве. *Международные процессы.* 2011, январь–апрель. Т. 9, № 1 (25). http://http://www.intertrends.ru/twenty-fifth/009.htm (последнее посещение — 30 августа 2012 г.).

[46] Там же.

[47] Положение интернета в Китае.

[48] Тарасенко П. Интернет загородят великой стеной. *Коммерсантъ.* 2012, 30 мая. № 96 (4881). http://http://www.kommersant.ru/doc/1946451 (последнее посещение — 30 августа 2012 г.).

[49] Цой А. Китайские блогеры обходят цензуру. *Telecom Blog*. 2012, 26 марта, http://telecomblog.ru/?p=10702 (последнее посещение — 30 августа 2012 г.).