Маркова Александра Вениаминовна

ОТНОШЕНИЯ КНР И США В ИНТЕРНЕТ-ПРОСТРАНСТВЕ В КОНТЕКСТЕ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ

В статье обозначены основные сходства и различия взглядов политического руководства США и КНР в сфере кибербезопасности. Исследование политики США и КНР в данной области, их опыта сотрудничества и споров представляется автору особенно важным в условиях появления новых вызовов и международных проблем, в том числе обострения угрозы международного терроризма. Все больше внимания информационной сфере, а именно кибербезопасности, уделяется со стороны российского руководства, что свидетельствует о возросшей роли киберпространства в современной мировой политике.

Адрес статьи: www.gramota.net/materials/3/2014/12-3/31.html

Источник

Исторические, философские, политические и юридические науки, культурология и искусствоведение. Вопросы теории и практики

Тамбов: Грамота, 2014. № 12 (50): в 3-х ч. Ч. III. С. 141-144. ISSN 1997-292X.

Адрес журнала: www.gramota.net/editions/3.html

Содержание данного номера журнала: www.gramota.net/materials/3/2014/12-3/

УДК 327.56
Политология

В статье обозначены основные сходства и различия взглядов политического руководства США и КНР в сфере кибербезопасности. Исследование политики США и КНР в данной области, их опыта сотрудничества и споров представляется автору особенно важным в условиях появления новых вызовов и международных проблем, в том числе обострения угрозы международного терроризма. Все больше внимания информационной сфере, а именно кибербезопасности, уделяется со стороны российского руководства, что свидетельствует о возросшей роли киберпространства в современной мировой политике.

Ключевые слова и фразы: КНР; США; Россия; информационная безопасность; кибербезопасность; киберпространство; Интернет; киберугрозы.

Маркова Александра Вениаминовна
Нижегородский национальный исследовательский университет им. Н. И. Лобачевского
aleksandra.markova@inbox.ru

ОТНОШЕНИЯ КНР И США В ИНТЕРНЕТ-ПРОСТРАНСТВЕ В КОНТЕКСТЕ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ©

Работа поддержана грантом (соглашение от 27 августа 2013 г. № 02.B.49.21.0003 между МОН РФ и ННГУ).

В современных условиях развития невозможно отрицать тот факт, что роль информационной среды неуклонно возрастает. Более того, информационная безопасность оказывает прямое влияние на все составляющие политики современного государства. Стремительное развитие информационных технологий приводит к тому, что миллиарды долларов, затраченные на оборону и различные виды вооружения, начиная от обычного и заканчивая ядерным, не оправдают себя, если будет достаточно запустить программу или вирус, чтобы нарушить работу всего оборонного комплекса страны.

Вместе с возрастанием роли информации в мировой политике повышаются риски, связанные с намерениями государственных и негосударственных акторов международной среды дестабилизировать информационную инфраструктуру того или иного государства. В подобных условиях разработка собственного подхода к обеспечению кибербезопасности является жизненно важной для современного государства. Актуальность изучения проблемы взаимоотношений государств в киберпространстве обусловлена также переходом от гонки в технических вооружениях в информационное поле, то есть развитием нового типа противостояния – информационной борьбы. В настоящее время происходит переход соперничества между США и Китаем в новое киберпространство, в силу чего необходимо обратить внимание на американский и китайский подход к формированию политики в области кибербезопасности.

Данная проблема была освещена в исследованиях российских ученых, среди которых мы хотели бы выделить работы Д. Балуева, А. Новоселова, М. Бескоровайного, Е. Зиновьевой и др. Однако, несмотря на пристальное внимание к киберпространству, стоит отметить, что эта проблема остается малоизученной и требует дополнительного рассмотрения для разработки практических рекомендаций российским лицам, принимающим решения.

США и Китай являются одними из самых влиятельных государств на мировой арене, что проявляется не только в экономической, военной или политической сферах, но также и в информационной политике двух государств. В США целые институты заняты разработкой новых способов ведения операций в киберпространстве и методов обороны от кибератак. В Китае подобные инициативы воплощаются по линии различных государственных ведомств и министерств, отвечающих за обеспечение государственной и военной безопасности страны (Министерство обороны и Министерство государственной безопасности). Кроме того, в структуре Народно-освободительной армии Китая имеются свои институты, занятые в области обеспечения кибербезопасности, – Главное политическое управление и Управление радиоэлектронной борьбы Генерального штаба НОАК.

С пришествием на пост президента Барака Обамы фактором, повлиявшим на информационную сферу политики государства, стал провал амбиций и планов на мировое лидерство. Теперь США стали развиваться по концепции «первый среди равных», хотя вопросы информационной безопасности остались приоритетными.

Охарактеризовать отношения между Китаем и США в информационной сфере весьма сложно. США и Китай являются самыми влиятельными государствами, и достижение консенсуса в области кибербезопасности необходимо для успешного развития не только Интернета, но и многих других отраслей, в том числе экономики, политики и обороны [6].

Принципиальное отличие позиций США и Китая в отношении киберпространства можно проследить в официальных взглядах правительств двух государств на обеспечение информационной безопасности, на которых строится внешняя и внутренняя политика. Согласно официальным американским документам и взглядам, США считают демократические принципы определяющими по отношению к государственной

политике. В свою очередь, Пекин не причисляет свободный доступ и обмен информацией к неотъемлемым правам человека и гарантиям построения стабильного общества.

США декларируют, что рассматривают кибербезопасность с точки зрения предоставления гарантий гражданам страны доступа к информации, условий для ее свободного обмена и генерирования. Так, в «Комплексной национальной инициативе по кибербезопасности» говорится, что «инициатива была разработана с большой заботой и вниманием к конфиденциальности и гражданским свободам в тесном сотрудничестве с правительственными экспертами по частной жизни. Защита гражданских свобод и права на частную жизнь остается фундаментальной целью в исполнении мер Инициативы» [10]. Стоит отметить, что при этом последние скандальные разоблачения США в прослушке телефонов, слежке и сборе информации о своих собственных гражданах прямо противоречат подобным заявлениям.

Китай считает, что открытый и свободный доступ к различного рода информации может стать угрозой для стабильности внутри страны. При формировании политики кибербезопасности правительство КНР обращает внимание на возросшую роль Интернета, увеличившуюся взаимозависимость государств в киберпространстве, потенциальные угрозы вторжения через киберпространство, а также на необходимость государства контролировать Интернет [6]. Причина такой политики состоит в беспокойстве Китая, что кибербезопасность затрагивает вопросы государственных и коммерческих тайн и личной жизни граждан. Кроме того, по мнению китайских экспертов, идеологическое измерение кибербезопасности должно отвечать целям распространения социалистической идеологии и культуры для поддержания стабильности в обществе [Ibidem].

По мнению американских ученых, стандарты защиты гражданских прав в США выше, чем в странах с авторитарными режимами, с которыми США сотрудничают по борьбе с терроризмом [2, с. 144]. С одной стороны, проблемная ситуация на интернет-рынке Китая отображает борьбу за влияние в киберпространстве между Китаем и США. С другой стороны, вышеуказанные различия исходят из противопоставления демократического режима авторитарному, что также можно увидеть на следующем примере.

С точки зрения руководства США, такие популярные сайты, как *Twitter* и *Youtube*, обеспечивают свободу слова и самовыражения, в то время как для Пекина они выступают в роли инструментов информационного влияния, навязывания западных ценностей [9]. В 2007 году Китай впервые заблокировал видеохостинг *Youtube* для защиты идеологической стабильности внутри государства, а окончательно сайт был заблокирован для китайских пользователей в 2009 г. Параллельно обостряется конфликт между Китаем и поисковой системой *Google*. Разногласия между компанией и китайским руководством возникли по вопросам цензуры, на которой настаивало последнее. Идеология *Google* полностью противоречит принципам китайского режима; Пекин считает, что цензура и государственное регулирование киберпространства не является нарушением прав и свобод человека, а, напротив, направлена на их защиту.

Руководством США и Китая был предпринят ряд инициатив для развития сотрудничества в данном направлении. В частности, во время визита госсекретаря США Джона Керри в Пекин была создана рабочая группа по вопросам кибербезопасности, которая создала механизм для диалога по кибербезопасности, что стало одной из первых попыток США наладить отношения с Китаем на фоне раскрытых Эдвардом Сноуденом данных о проводимом кибершпионаже против Китая со стороны Америки примерно с 2009 г.

К сожалению, сотрудничество в рамках работы рабочей группы было приостановлено после обвинений США против Китая в коммерческом шпионаже. Сообщения об этом появились в прошлом году, когда США заявили о попытке со стороны пяти китайских военных чиновников кражи коммерческих секретов с использованием новейших технологий. Американское обвинение указывает и на связь между НОАК и коммерческими китайскими компаниями. Например, США заявили, что крупная китайская компания по производству стали наняла чиновников Народно-освободительной армии, чтобы помочь создать базу данных для хранения украденной информации об американских разработках. Название компании не фигурировало в обвинительном заключении. Кроме того, американская технологическая и экономическая информация становится для других стран все более ценной, чем иная засекреченная информация [3, с. 7].

В свою очередь, Китай обвинил США в кибершпионаже, о чем также стало известно в мае 2014 г. Расследование случаев американского шпионажа в интернет-пространстве выявило, что Китай был главной целью во время ведения противозаконных операций со стороны США. Официальные представители китайской администрации заявили, что большинство атак ведется с территории США; по подсчетам китайских экспертов, в 2012 г. число атак составило более 34 тыс. [5].

Данный эпизод послужил доказательством того, что США вывели операции по шпионажу в киберпространстве за рамки борьбы с терроризмом и используют методы разведки в интернет-пространстве для удовлетворения «личных интересов», игнорируя при этом нравственный аспект дела и нарушая нормы международного права.

К этому стоит добавить, что защита национальных интересов с применением киберпространства не является основным направлением деятельности китайских хакеров. Пекин стремится дать толчок научно-техническому прогрессу, что, в свою очередь, заставляет активно работать научно-техническую разведку, используя для этого широкий спектр возможностей – традиционных и/или нетрадиционных (внедрение, подкуп, провокации) и новых. В этой связи для КНР принципиальное значение имеет приобретение инфраструктуры военного характера, но с применением исключительно в мирных целях, что отображается в сопутствующих документах. При этом Пекин допускает использование разных каналов с целью овладения информацией технического характера, раскрывающей военный потенциал разработок (от легальных – по дипломатической линии – до нелегальных) [7, p. 291].

По мнению китайских источников, США часто пренебрегают рамками суверенитета других государств в киберпространстве. Китай считает, что кибербезопасность для США используется, в первую очередь, для подавления конкурентов и поддержания американской безопасности, в то время как другие нации обязаны открыть свое интернет-пространство. Это не удивительно: по мнению лиц, принимающих решения в США, информация, полученная путем перехвата сообщений, передаваемых по различным каналам связи, в том числе и электронной почте, является весьма важной для борьбы с международным терроризмом [9]. Кроме того, Пекин справедливо отмечает, что право на частную жизнь американских граждан неприкосновенно для США, чего нельзя сказать об иностранцах, в том числе и жителях Китая. Таким образом, Китай убежден, что США проводят гонку вооружений в киберпространстве, что, безусловно, вредит двустороннему сотрудничеству.

Степень защищенности информационных систем двух государств также различна. Например, Китай, в силу технологического отставания, часто использует пиратское ПО для защиты компьютеров, что особенно распространено в коммерческой сфере; ситуация в США совершенно иная, где уже давно имеются собственные разработки по защите инфраструктуры от вторжения. Такое различие обуславливает взгляды США и КНР на построение международных правил и норм по кибербезопасности. С одной стороны, оба государства согласны, что без общепринятых норм поведения в Интернете дальнейшее международное сотрудничество в данном вопросе просто невозможно. С другой стороны, Пекин неоднократно предлагал создать широко представительную международную структуру, от чего США отказываются до сих пор.

Исходя из вышесказанного, российским лицам, принимающим решения в области кибербезопасности, следует исходить из следующих параметров.

Во-первых, в силу технической отсталости и печального опыта СССР в годы холодной войны есть основания полагать, что Пекин вряд ли вступит в открытую конфронтацию с США в вопросе обеспечения кибербезопасности. Однако наращивание мощностей в информационной сфере и способностей электронных атак может дать Пекину ощутимый перевес и приблизить вероятность поражения США. В данной связи Российской Федерации необходимо усилить меры внутриполитического характера по стимулированию развития технологической составляющей кибербезопасности для сохранения баланса сил и составления противовеса КНР и США в области кибербезопасности.

Во-вторых, можно прийти к выводу, что сотрудничество в сфере кибербезопасности будет осложнено деятельностью преступных групп и отдельных хакеров, ведущих деятельность против Китая с территории США и наоборот. Проблема состоит в сложности классификации угроз, исходящих с территории государства и непосредственно от него. Вследствие данной тенденции необходимо подчеркнуть необходимость для РФ выработки мер по идентификации киберугроз, а также их своевременного обнаружения и предотвращения.

Наконец, США и КНР продолжат принимать участие в международных инициативах по построению безопасности в киберпространстве, однако они вряд ли смогут пойти на уступки по определяющим вопросам, таким как взгляды США и КНР на свободу Интернета и информации. В силу подобных трендов российскому руководству необходимо подкрепить вышеуказанные мероприятия по обеспечению кибербезопасности внешним фактором, а именно развитием международного сотрудничества, в первую очередь с КНР как традиционным союзником на международной арене, в рамках данного политического направления.

Список литературы

1. **Зиновьева Е. С.** Компании интернет-индустрии как участники мировых политических процессов // Негосударственные участники мировой политики. М., 2013. С. 72-79.
2. **Поскребышева Е. С., Старкин С. В.** Внешнеполитическая стратегия «Союза правых сил» и прогнозы Национального разведывательного совета США: сравнительный анализ // Исторические, философские, политические и юридические науки, культурология и искусствоведение. Вопросы теории и практики. Тамбов: Грамота, 2011. № 2. Ч. 3. С. 144-148.
3. **Старкин С. В.** Анализ разведывательной информации по транснациональному терроризму в современных внешнеполитических условиях: подходы американских теоретиков // Гуманитарные исследования. 2011. № 1 (37). С. 6-11.
4. **Старкин С. В.** Проблемы типологизации разведывательной информации в американском теоретическом дискурсе // Вестник Нижегородского университета им. Н. И. Лобачевского. 2011. № 1. С. 329-335.
5. **China Demands Halt to 'Unscrupulous' US Cyber-Spying** [Электронный ресурс]. URL: http://www.theguardian.com/world/2014/may/27/china-demands-halt-unscrupulous-us-cyber-spying (дата обращения: 05.11.2014).
6. **Lieberthal K. G., Singer P. W.** Cybersecurity and U.S. – China Relations [Электронный ресурс]. URL: http://www.brookings.edu/research/papers/2012/02/23-cybersecurity-china-us-singer-lieberthal (дата обращения: 10.09.2014)
7. **Petukhov A. Y., Komarov I. D., Starkin S. S., Markova A. V.** Transition of Rivalry between USA and China to New Internet-Space // Advances in Environmental Biology. 2014. № 8 (13). P. 290-293.
8. **Riley M.** U.S. Charges against Chinese Hackers Cap Anti-Spying Push [Электронный ресурс]. URL: http://www.bloomberg.com/news/2014-05-20/u-s-charges-on-china-hackers-cap-3-year-pressure-drive.html (дата обращения: 15.08.2014).
9. **Swaine M. D.** Chinese Views on Cybersecurity in Foreign Relations Initiative [Электронный ресурс]. URL: http://carnegieendowment.org/email/South_Asia/img/CLM42MSnew.pdf (дата обращения: 25.07.2014).
10. **The Comprehensive National Cybersecurity Initiative** [Электронный ресурс]. URL: http://www.whitehouse.gov/sites/default/files/cybersecurity.pdf (дата обращения: 25.08.2014).
11. **Ting Shi, Riley M.** China Halts Cybersecurity Cooperation after U.S. Spying Charges [Электронный ресурс]. URL: http://www.bloomberg.com/news/2014-05-20/china-suspends-cybersecurity-cooperation-with-u-s-after-charges.html (дата обращения: 25.07.2014).

RELATIONS OF THE PEOPLE'S REPUBLIC OF CHINA AND THE USA IN NETWORK SPACE IN THE CONTEXT OF SECURING CYBER-SAFETY

Markova Aleksandra Veniaminovna
Lobachevsky State University of Nizhni Novgorod
aleksandra.markova@inbox.ru

The article identifies the basic similarities and differences in the views of the political leadership of the USA and the People's Republic of China in the sphere of cyber-safety. According to the author, investigating the policy of the USA and the People's Republic of China in this sphere, their experience of cooperation and conflicts is of special importance under the conditions of new challenges and international problems including the escalation of international terrorism. The Russian authorities pay more attention to information sphere, namely, cyber-safety, which testifies for the increased role of cyberspace in modern world politics.

Key words and phrases: The People's Republic of China; The USA; Russia; information safety; cyber-safety; cyberspace; Internet; cyber-dangers.

УДК 329
Политология

В статье рассматриваются методологические проблемы концептуализации политических партий в контексте трансформации российской партийной системы. Выявляются критерии, по которым политическая партия может быть идентифицирована в рамках категории «действия» как актор. Определены современные тенденции в исследовании политических партий. Отмечены «болевые точки» концептуализации политических партий. Выделены системные характеристики построения базы данных «Политические партии России в действии».

Ключевые слова и фразы: политические партии; акторы; политические акторы; партийная система; партийная реформа; методология исследования; политический субъект; база данных; акторно-сетевая теория.

Мартьянов Денис Сергеевич, к. полит. н.
Санкт-Петербургский государственный университет
dsmartyanov@mail.ru

Невзоров Максим Вадимович
Российский государственный педагогический университет им. А. И. Герцена
max.nevzorov@gmail.com

МЕТОДОЛОГИЧЕСКИЕ АСПЕКТЫ ИССЛЕДОВАНИЯ РОССИЙСКИХ ПОЛИТИЧЕСКИХ ПАРТИЙ КАК ПОЛИТИЧЕСКИХ АКТОРОВ. ЧАСТЬ I©

Статья подготовлена при поддержке гранта РГНФ 14-03-12012.

С апреля 2012 года были изменены правила создания политических партий в России, что привело к быстрому росту их числа. За два с половиной года в списке зарегистрированных партий Министерством Юстиции России побывало 88 политических партий, среди которых и двенадцать партий, в отношении которых внесена запись в ЕГРЮЛ о прекращении деятельности. Для исследования особенностей развития партийной системы в России на современном этапе развития был инициирован проект «Партии России в действии» по созданию базы данных, в которой собиралась бы количественная и качественная информация, описывающая партии. В целях повышения методологической целостности проекта мы задались двумя вопросами: «насколько политические партии в России являются партиями в полном смысле этого слова?» и «какова роль новых политических партий в российском политическом процессе?».

Как по проблеме изменения российской партийной системы в целом, так и по феномену новых партий в частности, на настоящий момент вышло не так много работ. Однако уже имеющиеся наработки указывают на три тенденции:

- во-первых, будет продолжено традиционное для отечественной политологии направление по изучению развития количественных аспектов партийной системы в рамках компаративистики. Так, в 2008 году Л. В. Сморгунов обратил внимание на необходимость рассмотрения феномена новых партий в контексте процесса электоральной подвижности [12];
- во-вторых, налицо скепсис в отношении складывающейся партийной системы. Подчеркивается роль рациональных акторов (не всегда политических) в создании партии, в том смысле, что последняя становится лишь «политическим проектом». Не только в публицистических, но и научных работах появляются новые дефиниции, которые отражают эту скрытую тенденцию: партии-спойлеры, франшизы, виртуальные и т.п. [8].