An Internet with BRICS Characteristics: Data Sovereignty and the Balkanisation of the Internet

Dana Polatin-Reuben
University of Oxford
dana.polatin-reuben@cs.ox.ac.uk

Joss Wright
University of Oxford, UK
joss.wright@oii.ox.ac.uk

July 7, 2014

Abstract

Data sovereignty, a catch-all term to describe different state behaviours towards data generated in or passing through national internet infrastructure, has become a topic of significant international debate in the wake of the Snowden revelations. A spectrum of approaches has emerged, with the United States and its allies viewing data 'localisation' as a threat to a free and open global internet and countries such as Russia, China and Brazil advocating for data sovereignty as a way of securing sensitive national data from foreign surveillance. This paper will examine BRICS-country approaches to data sovereignty, both by individual countries and as a group. Past participation by BRICS countries in internet governance forums will be examined, and a requirements analysis will be undertaken of data sovereignty needs. The risks posed by different interpretations of data sovereignty will be reviewed, with an assessment of whether the creation of a virtual 'BRICS bloc' would necessarily amount to full-scale internet Balkanisation.

1 Introduction

Data sovereignty has emerged as a contentious issue amongst the international community following revelations by Edward Snowden, published in *The Guardian* and other newspapers around the world, that the United States and its allies implemented a global mass surveillance programme. This has led to a debate about the global governance of the internet, made more pressing as the United States' National Telecommunications and Information Administration within the Department of Commerce recently announced its intent to 'transition key Internet domain name functions to the global multistakeholder community.' [1]

The term 'data sovereignty', while lacking a firm definition, refers to a spectrum of approaches adopted by different states to control data generated in or passing through national internet infrastructure. It can be understood as a subset of cyber sovereignty, defined as the subjugation of the cyber domain to local jurisdictions. Gourley recently pointed out that '[as] the cyber domain is an infrastructure with geographical ties, an artificial, man-made construct, each component is subject to the laws and jurisdiction of a sovereign authority.' [2]

While the assertion of cyber sovereignty may happen within the technical, social, judicial, or geopolitical spheres, data sovereignty refers specifically to the attempt by nation-states to subject data flows to national jurisdictions. Within this continuum exist the two poles of weak and strong data sovereignty. Weak data sovereignty as defined in this paper refers to private sector-led data protection initiatives with an emphasis on the digital-rights aspects of data sovereignty, whereas strong data sovereignty favours a state-led approach with an emphasis on safeguarding national security.

Global stakeholders have taken differing approaches to the issue of data sovereignty. The technical community responsible for maintaining the infrastructure of the global internet released the Montevideo Statement on the Future of Internet Cooperation in response to the Snowden revelations, warning against 'Internet fragmentation at a national level' and advocating the transition of governance to the multistakeholder community comprised of governments, the private sector, academia, and civil society [3]. Similarly, American stakeholders have warned against 'data localization' and 'erecting Schengen zones for data' [4]. However, American credibility as 'good stewards' has been so damaged by the Snowden revelations that even the European Union is considering adopting a local cloud to ensure protection of its sensitive data [5].

This paper will specifically examine approaches to data sovereignty taken by the BRICS countries - Brazil, Russia, India, China, and South Africa. With its first summit held in 2009, the BRICS consortium contains one third of the world's population and has an estimated $4 trillion in foreign reserves. They have acted as a bloc to challenge Western financial hegemony, most notably in beginning talks to form a new development bank which will rival the Western-dominated International Monetary Fund and World Bank [6].

Although much of the analysis presented relies on the concept of data sovereignty as an external frame for understanding national approaches to data policy, data sovereignty is also being actively pursued by some within the consortium, most notably Brazil, Russia, and China. Should the BRICS countries reach consensus on their requirements for data sovereignty, they could significantly shape the currently-occurring internet governance debate.

In Section Two, the past participation of BRICS countries within internet governance forums will be examined, followed by a national-level analysis of data sovereignty requirements based on current legislation and political discourse in Section Three. Section Four will discuss the likelihood of the BRICS countries achieving a Balkanising consensus, or a consensus which favours the creation of isolated national 'intranets' under the complete jurisdiction of the state. Finally, potential future work on this subject will be discussed in Section Five.

2 BRICS Countries and Internet Governance

BRICS-country participation in internet governance issues predates the formation of the bloc. All five countries participated in the World Summit on the Information Society, held in Geneva in 2003 and Tunis in 2005, and all were represented at the 2013 Internet Governance Forum meeting held in Bali. Most recently, all but South Africa participated in the High Level Government Meeting held at the 50th meeting of the Internet Corporation of Assigned Names and Numbers (ICANN). Additionally, the Brazilian Internet Steering Committee, in conjunction with /1Net, recently organised the Global Multistakeholder Meeting on the Future of Internet Governance (NETmundial) in São Paulo, which was the first internet governance meeting to explicitly invite the contributions of stakeholders from multiple segments of society.

While the BRICS countries do not have complete consensus on data sovereignty requirements, collaborations among the bloc have taken place. Notably, all BRICS countries but India signed the controversial Final Acts of the World Conference on International Telecommunications 2012, held in Dubai by the International Telecommunication Union (ITU) [7]. Of particular concern to countries who abstained from signing WCIT-12 was the non-binding language contained in Resolution 3, 'To foster an enabling environment for the greater growth of the Internet', which while not actively contradicting the multistakeholder model of internet governance appeared to assert sovereignty rights for member states and an active governance role for the ITU.

Brazil, China, and Russia have been particularly active on data sovereignty within the United Nations. In September 2011, the permanent representatives of China, Russia, Tajikistan, and Uzbekistan submitted a proposal to the UN General Assembly entitled 'International code of conduct for information security'

[8]. This voluntary code, which has thus far failed to reach consensus, asserts that 'policy authority for Internet-related public issues is the sovereign right of States' as opposed to other stakeholders. Additionally, other sovereign rights are asserted over data, such as the right to curb 'the dissemination of information that incites terrorism, secessionism or extremism' and the right 'to protect their information space and critical information infrastructure from threats, disturbance, attack and sabotage'.

Brazil, on the other hand, submitted a successfully adopted joint resolution with Germany in November 2013 following the Snowden revelations, entitled 'The right to privacy in the digital age' [9]. This resolution approaches data sovereignty as a human rights issue revolving around the violation of the right to privacy posed by mass surveillance. Rather than stress the sovereign rights of nations, the resolution requires states to implement effective oversight of their surveillance activities 'with a view to upholding the right to privacy and ensuring the full and effective implementation of all their obligations under international human rights law'.

3 Requirements Analysis

The data sovereignty requirements of individual BRICS countries, as stated in legislation and national discourse, are examined below in further detail.

3.1 Brazil

Although Brazil has been advocating for greater citizens' rights on the internet for some time, as with the recently-passed Marco Civil da Internet which first emerged in draft form in 2009, its national discourse surrounding data sovereignty has reached fever pitch post-Snowden. In November 2013, President Dilma Rousseff advocated for an amendment to the Marco Civil which would have required foreign cloud service providers to store Brazilian data on servers hosted in Brazil [10]. The final version of the bill included the less controversial provision that foreign cloud service providers operating within Brazil be beholden to Brazilian law [11].

Brazil has also been an active advocate for the multistakeholder model of internet governance, as evidenced by the organisation of NETmundial. Out of 187 contributions received, Brazilian stakeholders alone submitted 16 contributions [12]. Additionally, the Institute for Communication Research, based in Florianópolis, Brazil and Stuttgart, Germany, submitted a contribution, and the Society for Knowledge Commons, based in Brazil and India, submitted two contributions. In fact, NETmundial accepted contributions from stakeholders within all BRICS countries: China submitted two contributions from the government and the China Institutes of Contemporary International Relations (CICIR); India submitted five contributions from the government, private sector and non-profit organisations; Russia submitted three contributions, one from the government and two from the Russian Center for Policy Studies (PIR Center); and the Association for Progressive Communications (APC), with its executive director's office in South Africa, submitted two contributions.

The NETmundial outcome, reached by consensus, included a detailed section on human rights and shared values; a paragraph on limiting intermediary liability for end-user content; a declaration that the internet 'should continue to be a globally coherent, interconnected, stable, unfragmented, scalable and accessible network-of-networks'; and an endorsement of the multistakeholder model. This would suggest that Brazil is well-placed to act as an arbiter between the Western alliance, with its vision of a free and open internet, and countries such as China and Russia, whose concerns centre around safeguarding sensitive national data.

3.2 Russia

The Duma, Russia's parliament, has been considering questions related to data sovereignty for several years, with an increase in regulatory legislation following the 2012 re-election of President Vladimir Putin. Focus has been primarily on domestic regulation, with critics accusing the Kremlin of suppressing political dissidents. For instance, in July 2012 Putin signed into law the Internet Restriction Bill, which created the federation-wide Single Register of

websites blocked in Russia [13]. Although the law only specifies three categories of censored material - 'child pornography, instructions or propaganda for drug use, and material promoting suicide' - the law not only allows for other websites to be blocked by discretionary court order, but also blocks by IP address, which has led to the censoring of innocuous websites such as humour website Lurkmore [14]. In April 2014, the Duma also passed a law requiring bloggers with more than 3,000 daily readers to register with the Roskomnadzor, Russia's media oversight agency, thus eliminating their ability to remain anonymous [15][16].

Additionally, Russia's System of Operative-Investigative Measures, or SORM, has been conducting extensive domestic surveillance operations since the mid-1980s, according to a recent joint investigation by Agentura.ru, CitizenLab and Privacy International [17]. The use of SORM has increased following the mass protests against Putin's re-election campaign which erupted in December 2011.

Given the culturally protectionist language in its September 2011 joint UN proposal, and given its shared interest with China on curbing the influence of domestic separatists, it is clear that Russia's primary concern is the political control of information within its national borders. To that end, on 4 July 2014 the Duma passed a law reminiscient of the original draft of Brazil's Marco Civil requiring all Russian data to be stored on Russian servers by September 2016 [18]. The law still requires the approval of the upper chamber.

However, since 2011 Russia has also been updating its legislation on the processing of personal data to bring it into line with the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data [19][20][21]. This would suggest that political leadership acknowledges the economic benefits of adopting the data protection policies of its European neighbours, which may deter Russia from pursuing a national intranet on par with China's.

3.3 India

With India commanding 43% of the global business process outsourcing market for the information technology sector in 2005 [23], and business process outsourcing accounting for 1% of India's GDP in 2008 [22], India views data protection as vital for its economic interests. In April 2011, India's government updated the Information Technology Act 2000 to include several privacy-related amendments pertaining to data processing, including mandating that businesses which collect and store personal data have a privacy policy, obtain consent for the collection of data, and only share data with companies which maintain the same standard of data protection [24].

It is worth noting that India appears to be most interested in safeguarding the data of its Western investors, rather than asserting sovereignty over its own nationally-generated data. For instance, India and the United Kingdom entered into a 'cyber pact' in 2012 with the aim of protecting British data stored in Indian data centres [25]. Additionally, India's private sector has been actively debating issues of data sovereignty arising from the global adoption of the cloud services business model [26]. Given India's robust private sector and unreserved endorsement of the multistakeholder model, India is more likely to take a Western approach to data sovereignty than a Sino-Russian approach.

3.4 China

China is globally reknowned, both positively and negatively, for its national intranet. The Ministry of Public Security's Golden Shield Project, known colloquially as the Great Firewall, has facilitated the creation of a separate Chinese internet ecosystem through wide-ranging censorship of web content.

It is unsurprising that data sovereignty and non-interference in other nations' sovereign affairs is of paramount importance to the Chinese government. In a speech given to the Brookings Institution in September 2013, Foreign Minister Wang Yi stressed the need to contain 'any behavior that disrupts order in cyberspace and endangers cyber security' [27].

China's focus on mutual respect in cyberspace is

further analysed by Mueller:

> China steadfastly supports a traditional, sovereignty-based communications governance regime in the international arena. It prefers an international regime organized around treaty-based intergovernmental organizations that rely on one-country, one-vote distributions of power. When China uses the word 'democratic' in this context, it means one country, one vote. Its point of reference for 'democracy' is not the rights and interests of the individual citizen, but is equality among sovereign states. [28]

In addition to conducting global cyber espionage against a number of Western companies [29], China has also been the target of extensive NSA surveillance, including the creation of back doors in Huawei networks [30]. As a result, national discourse about data sovereignty has focused on safeguarding sensitive data from foreign surveillance.

However, rather than moving towards further cutting the national intranet off from the global network, China actually appears to be building bridges to the global internet and cautiously exploring a multistakeholder model. Evidence for this new Open Door Policy comes not only in the form of an ongoing national-level multistakeholder internet development conference [31] and the stop-start Track 2 Sino-US Cyber Security Dialogue [32], but also from the overtures which China has been making to Europe about collaboration within the cyber security realm. The multistakeholder governance model was discussed in the first meeting of the Sino-European Cyber Dialogue [33], and the Chinese government's own policy paper on the European Union expresses the desire to jointly 'promote the building of a peaceful, secure, open and cooperative cyberspace.' [34]

Most recently, at the 50th ICANN meeting in London, Mr Lu appeared to endorse a multistakeholder model of internet by referring to 'multi-participation' and outlining roles which different stakeholders could play in global internet governance [35]. Although China appears to desire a privileged role for state actors in internet governance, its increased engagement in multistakeholder discussions is a promising first step towards a global governance consensus.

3.5 South Africa

Although South Africa has the second-largest economy in Africa behind Nigeria, it has been late to join the cyber security debate, much less the data sovereignty debate. Cyber awareness is currently an endeavour pursued primarily by academia [36] and civil society, rather than by the South African government which only approved its National Cyber Security Policy Framework in March 2012 [37].

The South African government's non-participation in internet governance issues was recently seen at the 50th ICANN meeting, with South Africa not represented in a delegation of ten African nations. Additionally, the South African government did not submit contributions to NETmundial, despite stakeholder submissions from eight other African countries [12]. This would suggest that the South African government has yet to fully participate in the data sovereignty and governance debate on a national rather than regional level as part of a larger African contingent.

African countries have acted as a bloc to push for a multistakeholder governance model which stresses human rights, development, and access. For example, African stakeholders at NETmundial called for an internet which is 'affordable, multilingual and open to all without censorship or restraint.' [38]

4 A Balkanising Consensus?

A range of data sovereignty requirements can be seen within the BRICS consortium, with multiple interpretations of data sovereignty possible. China and Russia have the strongest interpretation of data sovereignty, which is seen as vital to protecting national culture as well as sensitive data; followed by Brazil which asserts that data sovereignty is a citizen's right; followed by India which is approaching data sovereignty primarily from a private-sector perspective that is similar to the Western approach; followed by South Africa, which is still formulating its approach to data sovereignty.

One can place the BRICS countries within Mueller's plot of national approaches to internet governance [39], divided into four quadrants by two axes. The first axis denotes whether the nation prefers a national or transnational approach to internet governance, whereas the second axis determines whether a hierarchical approach to internet governance is preferred over a free-association networking approach. China and Russia are clearly cyber-reactionaries preferring a hierarchical and national-level approach to internet governance; Brazil seems to prefer an approach of global governmentality wherein a hierarchy of governance is established among transnational institutions; and India and South Africa trend closer to the Western vision of denationalised liberalism, wherein governance decisions are transnational and left to free association.

If the BRICS countries achieve consensus in their approach to data sovereignty issues, they could emerge as a formidable bloc in the global internet governance debate. However, multiple interpretations of data sovereignty could emerge, which would affect the shape of the future debate. The consequences of adopting a weak or strong approach to data sovereignty are discussed below.

4.1 Weak and Strong Data Sovereignty

A weak approach to data sovereignty is the more likely consensus, given the spectrum of approaches currently seen within the BRICS consortium. This approach would favour private sector-led data protection initiatives as well as an emphasis on the digital-rights aspects of data sovereignty.

Weak data sovereignty would require both Russia and China to give ground on issues of cultural protection in order to maintain economic competitiveness. However, even with more permeable national intranets, neither country is expected to approach data sovereignty with the same human-rights focus on individual freedoms which the West endorses, as opposed to social stability used as the justification for widespread censorship. One risk posed by a weak approach to data sovereignty is that global governance and development lists too heavily towards denationalised liberalism, neglecting to develop internationally-respected human rights norms.

Challenging as a weak approach to data sovereignty would be, the emergence of a consensus amongst the BRICS countries favouring a strong approach would pose even more risks. This would create a BRICS bloc directly opposed to the Western consensus, which would lead to global governance issues.

Not only would a strong approach to data sovereignty provide a pretext for expanding censorship activities within individual BRICS countries at the expense of privacy and freedom of expression, but the assertion of national sovereignty in the cyber sphere could lead to the escalation of hostilities in physical space as well. America's International Strategy for Cyberspace, released in May 2011, states that the United States '[reserves] the right to use all necessary means - diplomatic, informational, military, and economic ... to defend our Nation, our allies, our partners, and our interests.' [40] Should countries such as Russia and China also adopt this approach, it significantly raises the stakes of a cyber attack to include kinetic force.

Economically, strong data sovereignty would have severe implications for the global private sector. Given that American companies are obligated by United States law to share data stored on foreign servers with US law enforcement agencies [41], an assertion of sovereignty over data stored in a national jurisdiction could result in new barriers to operating an international cloud computing service. This would have far-reaching consequences beyond the information technology sector - any business which processes personal data would be affected, making business process outsourcing untenable. Additionally, the financial sector would have difficulty undertaking transactions across national borders.

4.2 The Challenge of Consensus

Though a strong approach to data sovereignty poses a threat to the organic development of a free and open global internet on a policy level, the enforcement of borders in cyberspace is not only practically infeasible architecturally, but also undesirable economically.

Given that the internet's core routing protocols do

not, in general, support source routing, any strategy relying on exercising meaningful control over the route taken by traffic flows is unlikely to be technically viable. A completely isolated national intranet is theoretically possible but would suffer greatly from problems of scale, not to mention economic and social difficulties. Sufficiently robust cyber powers also have the ability to compromise the data sovereignty of adversaries by installing interception devices outside of their official jurisdiction, as was seen with the United Kingdom's Tempora programme [42].

Even China, which is seen as the paragon of internet Balkanisation, is not impervious to the economic necessity of maintaining a globally-connected network. Complete data sovereignty would mandate the banishment of multinational cloud service providers from the national market, which would severely hamper trade and collaboration with other countries. Brazilian legislators had to revise the language of the Marco Civil da Internet such that foreign cloud service providers were merely beholden to Brazilian law, rather than the original unenforceable language which mandated that foreign companies store Brazilian data on servers located in Brazil [11]. The final language still risks being unenforceable in instances where the law within a foreign company's home nation contradicts Brazilian law.

Despite the evolution of the internet from 'a technology that resists territorial law to one that facilitates its enforcement' [43], full Balkanisation of the internet into regional intranets not only looks unlikely, but is not a desirable outcome even amongst the most outspoken proponents of data sovereignty within the BRICS countries.

5 Future Work

It is hoped that this paper will open up several avenues for related future research. An ongoing analysis of individual and collective BRICS-country approaches to internet governance issues will aid understanding as the global internet governance debate continues. Additionally, this analysis could be expanded to include G-20 economies as well as other developing nations.

Should a consensus on data sovereignty emerge from within the BRICS bloc, these requirements could be compared with current internet protocols to assess their technical feasibility. The likelihood of modifying internet protocols to support data sovereignty requirements could also be examined.

References

[1] National Telecommunications and Information Administration, 2014. "NTIA Announces Intent to Transition Key Internet Domain Name Functions." (online) 14 March. Available at: `http://www.ntia.doc.gov/press-release/2014/ntia-announces-intent-transition-key-internet-domain-name-functions` (Accessed 13 May 2014)

[2] Gourley, S. K., 2014. "Cyber Sovereignty." In: P. A. Yannakogeorgos and A. Lowther, eds. 2014. *Conflict and Cooperation in Cyberspace: The Challenge to National Security*. Boca Raton, Florida: Taylor & Francis. Chapter 16.

[3] Internet Corporation for Assigned Names and Numbers, 2013. "Montevideo Statement on the Future of Internet Cooperation." (online) 7 October. Available at: `https://www.icann.org/en/news/announcements/announcement-07oct13-en.htm` (Accessed 13 May 2014)

[4] Chander, A., and Le, U. P., 2014. "Breaking the Web: Data Localization vs. the Global Internet." *Emory Law Journal*, forthcoming; UC Davis Legal Studies Research Paper No. 378, 14 April. Available online at: `http://ssrn.com/abstract=2407858` (Accessed 13 May 2014)

[5] Hughes, K., and Grebler, D., 2014. "U.S. knocks plans for European communication network." *Reuters*, (online) 4 April. Available at: `http://www.reuters.com/article/2014/04/04/us-usa-trade-telecomunications-idUSBREA331W820140404` (Accessed 13 May 2014)

[6] Smith, D., 2013. "Brics eye infrastructure funding through new development bank." *The Guardian*, (online) 28 March. Available at: http://www.theguardian.com/global-development/2013/mar/28/brics-countries-infrastructure-spending-development-bank (Accessed 30 June 2014)

[7] International Telecommunication Union, 2012. *Final Acts of the World Conference on International Telecommunications*. Dubai, United Arab Emirates, 3-14 December 2012. Available online at: http://www.itu.int/dms_pub/itu-s/opb/conf/S-CONF-WCIT-2012-PDF-E.pdf (Accessed 12 May 2014)

[8] United Nations General Assembly, 2011. *Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General* (A/66/359), 12 September. Available online at: http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N11/496/56/PDF/N1149656.pdf?OpenElement (Accessed 11 May 2014)

[9] United Nations General Assembly, 2013. *The right to privacy in a digital age* (A/C.3/68/L.45), 1 November. Available online at: http://daccess-dds-ny.un.org/doc/UNDOC/LTD/N13/544/07/PDF/N1354407.pdf?OpenElement (Accessed 11 May 2014)

[10] Watts, J., and Kaiser, A., 2013. "Brazil to legislate on online civil rights following Snowden revelations." *The Guardian*, (online) 1 November. Available at: http://www.theguardian.com/world/2013/nov/01/brazil-legislate-online-civil-rights-snowden (Accessed 11 May 2014)

[11] Renâ, P., 2014. "Marco Civil da Internet unofficial english translation." *Cultural Digital e Democracia*, (blog) 28 March. Available at: http://thecdd.wordpress.com/2014/03/28/marco-civil-da-internet-unofficial-english-translation/ (Accessed 11 May 2014)

[12] Brazilian Internet Steering Committee and /1Net, 2014. "Contributions already submitted." *Global Multistakeholder Meeting on the Future of Internet Governance*. São Paulo, Brazil, 23-24 April 2014. Available online at: http://content.netmundial.br/docs/contribs (Accessed 12 May 2014)

[13] Nielsen, R., 2012. "Duma to Hear Internet Restriction Bill." *The Moscow Times*, (online) 4 July. Available at: http://www.themoscowtimes.com/sitemap/paid/2012/7/article/duma-to-hear-internet-restriction-bill/461555.html (Accessed 11 May 2014)

[14] J.Y., 2012. "Internet censorship in Russia: Lurk no more." *The Economist* Eastern approaches, (blog) 16 November. Available at: http://www.economist.com/blogs/easternapproaches/2012/11/internet-censorship-russia (Accessed 11 May 2014)

[15] Russian Presidential Executive Office, 2014. "Amendments to legislation introducing responsibility for spreading information via the Internet." (online) 5 May. Available at: http://eng.kremlin.ru/acts/7126 (Accessed 11 May 2014)

[16] Robertson, A., 2014. "Putin signs law forcing bloggers to register with Russian media office." *The Verge*, (online) 7 May. Available at: http://www.theverge.com/2014/5/7/5690410/putin-signs-law-forcing-bloggers-to-register-with-russian-media-office (Accessed 11 May 2014)

[17] Soldatov, A., and Borogan, I., 2013. "Russia's Surveillance State." *World Policy Journal*, Fall 2013. Available online at: http://www.worldpolicy.org/journal/fall2013/Russia-surveillance (Accessed 11 May 2014)

[18] British Broadcasting Corporation, 2014. "Russian MPs back law on internet data storage." *BBC News*, (online) 5 July. Available at: http://www.bbc.co.uk/news/world-europe-28173513 (Accessed 7 July 2014)

[19] Russian Presidential Executive Office, 2011. "Presidential instructions following meeting with internet community representatives." (online) 2 June. Available at: http://eng.kremlin.ru/news/2315 (Accessed 11 May 2014)

[20] Russian Presidential Executive Office, 2011. "Amendments to law on personal data." (online) 26 July. Available at: http://eng.kremlin.ru/news/2642 (Accessed 11 May 2014)

[21] Russian Presidential Executive Office, 2013. "Amendments to a number of laws on processing of personal data." (online) 8 May. Available at: http://eng.kremlin.ru/acts/5387 (Accessed 11 May 2014)

[22] Reuters, 2008. "India's outsourcing revenue to hit $50 bn." *The Financial Express*, (online) 29 January. Available at: http://www.financialexpress.com/news/indias-outsourcing-revenue-to-hit-50-bn/266661/1 (Accessed 13 May 2014)

[23] PricewaterhouseCoopers, 2005. *The Evolution of BPO in India*. (online) April 2005. Available at: http://www.pwc.in/en_IN/in/assets/pdfs/evolution-of-bpo-in-india.pdf (Accessed 13 May 2014)

[24] Ministry of Communications and Information Technology, 2011. "Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011." *The Gazette of India*, 11 April. Available online at: http://deity.gov.in/sites/upload_files/dit/files/GSR313E_10511%281%29.pdf (Accessed 13 May 2014)

[25] Kirkup, J., 2012. "David Cameron to strike cybercrime deal with India." *The Telegraph*, (online) 19 February. Available at: http://www.telegraph.co.uk/news/politics/9879272/David-Cameron-to-strike-cybercrime-deal-with-India.html (Accessed 13 May 2014)

[26] RP, S., 2014. "Data sovereignty in an era of cloud." *InformationWeek*, (online) 12 May. Available at: http://www.informationweek.in/informationweek/news-analysis/295770/sovereignty-era-cloud (Accessed 13 May 2014)

[27] Wang Yi, 2013. "Toward a New Model of Major-Country Relations Between China and the United States." The Brookings Institution, (speech) 20 September. Available online at: http://www.china.org.cn/chinese/2013-09/23/content_30101644.htm (Accessed 13 May 2014)

[28] Mueller, M. L., 2011. "China and Global Internet Governance: A Tiger by the Tail." In: R. Deibert, J. Palfrey, R. Rohozinski and J. Zittrain, eds., 2011. *Access Contested: Security, Identity and Resistance in Asian Cyberspace*. Cambridge, Massachusetts: MIT Press. Chapter 9. Available online at: *http://access.opennet.net/wp-content/uploads/2011/12/accesscontested-chapter-09.pdf* (Accessed 2 July 2014)

[29] Mandiant, 2013. *APT1: Exposing One of China's Cyber Espionage Units*. pdf 18 February. Available online at: http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf (Accessed 7 July 2014)

[30] Pengelly, M., 2014. "NSA targeted Chinese telecoms giant Huawei report." *The Guardian*, (online) 22 March. Available at: http://www.theguardian.com/world/2014/mar/22/nsa-huawei-china-telecoms-times-spiegel (Accessed 13 May 2014)

[31] Internet Society of China, 2014. "The 2014 China Internet Conference to be held in August." (online) 31 March. Available at: http://www.isc.org.cn/english/Focus/listinfo-29133.html (Accessed 13 May 2014)

[32] Center for Strategic and International Studies, 2014. "China Institute of Contemporary International Relations (CICIR)." (online) Available at: http://csis.org/program/china-institute-contemporary-international-relations-cicir (Accessed 13 May 2014)

[33] China Institutes of Contemporary International Relations, 2014. "1st Meeting of the Sino-European Cyber Dialogue." (online) 8 April. Available at: http://www.cicir.ac.cn/english/newsView.aspx?nid=5880 (Accessed 13 May 2014)

[34] The People's Republic of China, 2014. *China's Policy Paper on the EU: Deepen the China-EU Comprehensive Strategic Partnership for Mutual Benefit and Win-win Cooperation.* Beijing, China, 2 April. Available online at: http://www.china.org.cn/chinese/2014-04/02/content_31981279.htm (Accessed 13 May 2014)

[35] Internet Corporation for Assigned Names and Numbers, 2014. "LONDON - High Level Government Meeting." *ICANNFIFTY.* (transcript) London, United Kingdom, 23 June. Available online at: https://london50.icann.org/en/schedule/mon-1015-hlgm/transcript-hlgm-1015-23jun14-en.pdf (Accessed 1 July 2014)

[36] South African Cyber Security Academic Alliance, 2014. "Welcome to SACSAA." (online) Available at: http://www.cyberaware.org.za/ (Accessed 13 May 2014)

[37] United Nations Institute for Disarmament Research, 2013. *The Cyber Index: International Security Trends and Realities.* (pdf) Geneva: UNIDIR. Available at: http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf (Accessed 13 May 2014)

[38] Jere, T., 2014. "African Stakeholders' Contribution to NetMundial." *Global Multistakeholder Meeting on the Future of Internet Governance.* São Paulo, Brazil, 23-24 April 2014. Available online at: http://content.netmundial.br/contribution/african-stakeholders-contribution-to-netmundial/171 (Accessed 12 May 2014)

[39] Mueller, M. L., 2010. "Ideologies and Visions." In: M. L. Mueller, 2010. *Networks and States: The Global Politics of Internet Governance.* Cambridge, Massachusetts: MIT Press. Chapter 11.

[40] The White House, 2011. "International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World." (online) May 2011. Available at: http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (Accessed 2 July 2014)

[41] Gibbs, S., 2014. "US court forces Microsoft to hand over personal data from Irish server." *The Guardian*, (online) 29 April. Available at: http://www.theguardian.com/technology/2014/apr/29/us-court-microsoft-personal-data-emails-irish-server (Accessed 2 July 2014)

[42] MacAskill, E., Borger, J., Hopkins, N., Davies, N., and Ball, J., 2013. "Mastering the internet: how GCHQ set out to spy on the world wide web." *The Guardian*, (online) 21 June. Available at: http://www.theguardian.com/uk/2013/jun/21/gchq-mastering-the-internet (Accessed 13 May 2014)

[43] Goldsmith, J., and Wu, T., 2006. *Who Controls the Internet?: Illusions of a Borderless World.* Oxford: Oxford University Press.