Sovereign Data

THESIGERS

BRICS set out vision for international information security

The forthcoming BRICS summit will articulate a new collective vision of global information security but there are reasons to doubt its viability as a united front.

In July 2015, the BRICS group – Brazil, Russia, India, China and South Africa – will meet in the Russian Republic of Bashkortostan for its seventh annual summit. Under Russian presidency, the BRICS agenda will reflect common concerns about global political and economic affairs, as well as the specific strategic ambitions of its members.

One key area in which the BRICS group aims to make an international impact is information security. A new collective vision of 'international information security' (IIS) is emerging from pre-summit meetings and diplomatic statements – part turf war, part muscle-flexing riposte to a United States damaged by the Snowden affair.

Sovereign Data assesses these developments and finds that there are serious disagreements between BRICS countries about the meaning and future contours of internet governance. If these differences cannot be resolved, the prospects for a truly unified and credible BRICS information security project will be limited.

Background

BRICS group members are no strangers to information security issues, but speaking in unison on the topic is a new development. The Russian presidency states that BRICS has become an influential global actor with 'its own voice' on security issues. Information security cooperation may have been lacking historically but Russia notes that IIS is one of two areas (the other being regional conflicts) where BRICS cooperation has advanced the most. The ambition is for BRICS to become a global player in information security and internet governance.[1] This reaffirms the 'paramount importance' attached to the security of information and information technologies at previous BRICS summits and the role of BRICS in developing legal, behavioural and normative change in this key policy field.

In May 2015, BRICS national security advisors agreed to prepare 'common approaches to information security', informed by a reformed system of global governance that promotes 'cooperative, equal, and indivisible security'.[2] This modifies the 2013 BRICS commitment to a 'peaceful, secure, and open cyberspace'.[3] There is also a toning-down of the 2014 diplomatic language that criticised the United States for the mass surveillance and data collection activities of its intelligence services.

The Fortaleza Declaration of July 2014, for instance, framed this activity as the 'violation of the sovereignty of States and of human rights'.[4] In the wake of the Snowden disclosures Brazil's president Rouseff excoriated the US before the UN General Assembly and has been at the forefront of international condemnation of US intelligence policy and practice.[5] Brazil and its BRICS allies have even planned to lay their own internet cables to avoid routing internet traffic through the United States.[6] In 2015, the BRICS articulate only the desire to 'internationalise' internet governance, a less obviously disputatious salvo against American dominance.[7]

Citation: "BRICS set out vision for International Information Security," *Sovereign Data* Vol 1. No. 1 (July 2015).

--

Keywords: BRAZIL, BRICS, CHINA, INDIA, INFORMATION SECURITY, INTERNET GOVERNANCE, RUSSIA, SOUTH AFRICA.

--

Explanation of dates:
Drafted: 2015-05-29
Information cut-off: 2015-06-18
Published: 2015-07-01

--

Editor: Dr. Tim Stevens
Email: editorial@thesigers.com

Sovereign Data is a monthly journal of politics, data and risk in emerging markets.

ISSN: 2059-075X

Published by Thesigers, the research and advisory firm. Thesigers is a trading name of Thesiger & Company Limited.

Address: 37 Great Russell Street,
London, WC1B 3PP, England.

Contacts:
Office (UK): +44 (0)134 430 6541
Email: enquiries@thesigers.com
Web: thesigers.com/publications

The BRICS group has always sought to challenge the hegemony of the United States in global affairs. In 2009 it transformed from an abstract economic category into a self-identifying political group, enabling its challenge to Western neoliberal capitalism and the economic crisis.[8] Recent declarations support this interpretation of BRICS intent. The BRICS group means to create 'a multipolar system of international relations based on the principles of justice and equality … laying the old practices of bloc diplomacy to rest'.[9] Russia's aim is to transform BRICS into 'a full-scale mechanism for strategic and day-to-day cooperation on key issues of world politics and global economy'.[10]

There are tensions that belie the apparent unity of this emerging geopolitical bloc. Since its creation, the heterogeneity of the states that make up the BRICS group suggests that its ability to articulate, let alone achieve, any 'meaningful vision for the future' is limited.[11] A closer assessment of the emerging BRICS information security agenda reveals that there is significant internal variation in the ways BRICS members understand and articulate key concepts and ideals. This could impact on the ability of BRICS to achieve stated ambitions.

Since its creation, the heterogeneity of the states that make up the BRICS group suggests that its ability to articulate, let alone achieve, any 'meaningful vision for the future' is limited

Behind the façade

The BRICS countries have divergent conceptions of sovereignty and cyberspace. These differences have less to do with technical information security – or 'cyber' security – than with the central question of internet governance: who should rule the internet? Each of the BRICS countries' position on the issue is defined by the relationship between two things: first, the role of the state in internet governance; and second, how much and what kind of formal organisation is needed to solve problems of internet governance.[12]

The former rests on the extent to which the internet should be subject to national sovereignty or considered a global domain. For the latter, there are two extremes: a hierarchical (and hence coercive) approach to internet governance, or a more distributed, networked arrangement for decision-making. This framework allows for a great number of variations, but each of the BRICS countries can be described in terms of one of four basic types.[13]

China and Russia, for example, are 'cyber-reactionaries', conservative entities aligning internet governance with state jurisdiction. This promotes the supremacy of national institutions and mechanisms over the internet, and preserves greatest freedom of movement for the state in domestic and foreign policy. Information security is closely identified with national security and the preservation of national identity and culture. It therefore takes on an explicitly nationalist tone usually absent, for example, in formulations of 'cyber security'. Information refers not only to data but to ideas and cultural contaminants damaging to the national body politic.

China and Russia support each other's ambitions, recently reaffirming their bilateral cooperation on 'network and information security', and pledging to respect the other's 'choice of developmental path conforming to its national conditions'.[14] This links national sovereignty tightly to control and authority over internet content and activities, including censorship. Cyber-reactionary states work through inter-governmental organisations where necessary, in order to promote this form of internet governance. In the case of China and Russia, this includes the Shanghai Cooperation Organisation (SCO) and the International Telecommunications Union (ITU), a UN agency.

Brazil prefers a 'global governmentality' approach, which also requires hierarchical control of the internet but by transnational institutions rather than states. Brazil led the Global Multistakeholder Meeting on the Future of Internet Governance (NETmundial) in April 2014. This was attended by delegates from governments, private sector, academia, civil society and non-profit organisations, and drafted broad-based principles for internet governance and proposed a roadmap for their implementation.[15]

India and South Africa are proponents of 'denationalised liberalism', in which individual actors govern the internet via transnational decision-making frameworks. This is a peer- and market-based approach that restricts hierarchical interventions to policing and national security functions. India's position can be attributed to its status as a leader in the global market in outsourced information technology. Growth has slowed in recent years but outsourcing remains a key sector of Indian industry and a crucial source of foreign currency.[16]

These descriptions suggest key areas of potential disagreement in the midst of an intensely complex situation. Given the risk of fracture, what are the prospects for a workable BRICS consensus on global information security?

Implications

The potential emergence of a BRICS information security project is not a response to US dominance alone. It is also an attempt to broker new consensus where none currently exists. There is no globally binding agreement on information security or internet governance, and the entities that exert control and authority are non-governmental organisations like ICANN that have evolved in ad hoc fashion along with the internet itself.[17] In broad terms, agreements have foundered on the simple fact that the US has seen no need for them. Without US buy-in, no global regime for internet governance is either likely to take hold or enforceable in practice. The US prefers an 'open internet' approach to facilitate commerce and cultural exports, even if its military and intelligence activities indicate that national security is often its overriding consideration. It also supports the globalisation of some internet governance functions historically closely tied to the US government.[18]

Opposition to the US model has come principally from Russia and China and other members of the SCO, particularly the SCO's International Code of Conduct for Information Security (2011), updated in 2015.[19] Lesser proposals have come from the IBSA sub-grouping (India, Brazil, South Africa), rooted in documents on global 'information society' like the 2003 Brasilia Declaration.[20] BRICS countries have tended to operate via either the SCO or IBSA, rather than in concert. Analysts identify the split between the SCO and Western democracies but less attention is paid to divisions within the BRICS group, in which there are deep-rooted differences between Russia and China on the one hand and the IBSA countries on the other.[21]

Under these conditions, the prospects of a BRICS consensus on internet governance and security look limited. While Russia and China pursue robust bilateral security agreements, questions are being raised in South Africa about intensifying ties with China on information security issues.[22] Brazil has no wish to damage good relations with the US, not least as their respective national priorities for the internet are so closely aligned. India has more to lose than gain by adopting restrictive models of internet governance. So too China, which reaps enormous economic benefit from its connections to the global internet. It may be that cooperation in this policy space is limited by the same factors that have always hampered it: ingrained differences in culture and outlook; intra-BRICS competition; and the strategic importance of the United States to all members.[23]

It may be that cooperation in this policy space is limited by the same factors that have always hampered it: ingrained differences in culture and outlook; intra-BRICS competition; and the strategic importance of the United States to all members.

Outlook

How the BRICS balance these competing visions of the future internet depends on how well its members navigate the role of the state in internet governance. Three of the BRICS 'group of five' converge intuitively with US views, which priorities Russia and China as traditional strategic foes. Such polarisation may be an insurmountable obstacle to consensus, at least in any framework that possesses the necessary bite to convince other governments and stakeholders to follow the BRICS lead. If they cannot muster this support, the BRICS proposals will look somewhat underpowered and are likely to fail. BRICS is not looking for radical change in the global order but the challenge before it is to engender any change at all.

NOTES

1. 'Concept of the Russian Federation's Presidency in BRICS in 2015-2016', 10 April 2015, http://russianunesco.ru/uploads/2015/04/17/Press-release_15_04_2015_RUISSIAN_PRESIDENCY_CONCEPT_1.pdf [accessed 18 June 2015].
2. 'Meeting of BRICS National Security Advisors Concludes in Moscow', 26 May 2015, http://en.brics2015.ru/news/20150526/117948.html [accessed 18 June 2015].
3. eThekwini Declaration, 27 March 2013.
4. Fortaleza Declaration, 15 July 2014.
5. Dilma Rouseff, statement before the 68th session of the UN General Assembly, New York, 24 September2013, http://gadebate.un.org/sites/default/files/gastatements/68/BR_en.pdf [accessed 18 June 2015].
6. 'Brazil begins laying its own Internet cables to avoid US surveillance', *The Washington Post*, 3 November 2014. See also, 'Brics cable unveiled for direct and cohesive communications services between Brazil, Russia, India, China and South Africa', *Business Wire*, 16 April 2012.
7. 'Concept of the Russian Federation's Presidency'.
8. Radhika Desai, 'The Brics are building a challenge to western economic supremacy', *The Guardian*, 2 April 2013.
9. 'Meeting of BRICS national security advisors'.
10. 'Concept of the Russian Federation's Presidency'.
11. Andrew S. Weiss, 'BRIC-à-brac', *Foreign Policy*, 15 June 2009, http://foreignpolicy.com/2009/06/15/bric-a-brac/ [accessed 18 June 2015].
12. Milton L. Mueller, *Networks and States: The Global Politics of Internet Governance* (Cambridge, MA: The MIT Press, 2010), pp. 255-9.
13. Dana Polatin-Reuben and Joss Wright, 'An internet with BRICS characteristics: Data sovereignty and the balkanisation of the internet', *4th USENIX Workshop on Free and Open Communications on the Internet*, San Diego, CA, 18 August 2014.
14. Ministry of Foreign Affairs of the People's Republic of China, 'Yang Jiechi attends 11th Round of the China-Russia Security Consultation', 26 May 2015, http://www.fmprc.gov.cn/mfa_eng/zxxx_662805/t1267292.shtml [accessed 18 June 2015].
15. http://netmundial.br/ [accessed 18 June 2015].
16. Tholons, *2015 Top 100 Outsourcing Destinations*, December 2014, http://www.tholons.com/nl_pdf/Tholons_Whitepaper_December_2014.pdf [accessed 18 June 2015].; 'Manila eclipses Mumbai as services outsourcing magnet', *Financial Times*, 5 May 2015.
17. Internet Corporation for Assigned Names and Numbers.
18. 'US government pulls out of ICANN', *IDG News Service*, 14 March 2014.
19. 'SCO member countries propose updated cyber security draft rules to UN', *Xinhua*, 10 January 2015.
20. Brasilia Declaration, Brasilia, 6 June 2003,

http://ibsa.nic.in/brasil_declaration.htm [accessed 18 June 2015].

21. Hannes Ebert and Tim Maurer, ‘Contested cyberspace and rising powers’, *Third World Quarterly* 34, no. 6 (2013): 1054-74.

22. Marian Shinn, ‘South Africa: Alarm over cyber security pact with China’, 10 June 2015’, http://allafrica.com/stories/201506101374.html [accessed 18 June 2015].

23. Michael A. Glosny, ‘China and the BRICs: a real (but limited) partnership in a unipolar world’, *Polity* 42, no. 1 (2010): 100-129.

ABOUT SOVEREIGN DATA

Sovereign Data is a Thesigers initiative focused on the “know-ability” of information and its influence on contemporary political and market processes. Thesigers defines “sovereign” and “data” broadly, in order to more fully understand the risks and opportunities associated with knowledge in all its tributary forms – “information”, “data”, “evidence”, “intelligence”, and so on.

Thesigers’ view of sovereign data is that it contains essential elements of substance and form, of meaning and context, akin to the way historians think of “primary sources” as original, often perishable artefacts of recorded information about people, places, events, issues and things.

--

Monthly Journal

Thesigers’ monthly journal, *Sovereign Data*, provides short, digestible analysis of the state of the information environment. Each monthly issue focuses on a single, current topic selected by Thesigers staff, given additional context and assessed for relevance and impact.

--

Reporting Service

Thesigers’ reporting service tracks current developments in sovereign data. Intended for clients who need more frequent, detailed updates, the service features summary reports and briefings based on locally-sourced news, data analytics, risk indexes and regular assessment.

—

Research and Development

Thesigers’ conducts ongoing research and development through a sense-making program of workshops, system design and technology innovation. Workshops investigate problems covered in our reporting and analysis. Our systems and technology work creates working solutions to them.

--

HOW TO SUBSCRIBE

Sovereign Data is published monthly and distributed direct to subscribers via email as a PDF attachment. Subscribers to the Reporting Service benefit from daily, weekly and monthly reporting and analysis. Subscription rates are based on frequency of reporting, subject matter coverage, depth of analysis and mechanism of delivery.

To discuss requirements and receive a quote, please contact us directly at

subscriptions@thesigers.com

Sovereign Data

THESIGER & COMPANY LIMITED
37 Great Russell Street, London, WC1B 3PP, England.
Registered in England and Wales (No. 07234402) VAT No. GB 135658985
Email: enquiries@thesigers.com Web: thesigers.com