BRICS Cybersecurity Cooperation: Achievements and Deepening Paths

Gao Wanglai

The year 2017 marked the beginning of the second decade of BRICS cooperation. Amidst the profound changes in the international security system, the BRICS mechanism has transformed from a forum focusing on economic governance toward a comprehensive cooperation mechanism that gives equal importance to political and economic governance. Due to imperfections in the international institutions and rules of the current global cyber governance, the rivalries among major powers and international organizations for the power to formulate the rules for cyberspace are heating up. The advancement in BRICS cybersecurity cooperation will help raise the voice of the developing countries in global cyberspace governance and the formation of a new order in global cyberspace.

Strategic Foundation for BRICS Cybersecurity Cooperation

The BRICS countries are all emerging economies, and they face common opportunities and challenges in cyberspace, which sets a solid strategic foundation for their cybersecurity cooperation.

Confronting common cybersecurity threats

The BRICS members are confronted with three common cybersecurity threats. The first is vulnerable information infrastructure. In recent years, their

Gao Wanglai is Associate Professor at the Institute of International Relations, China Foreign Affairs University (CFAU).

critical information infrastructure (CII) such as finance, electricity, transportation and energy systems have been the major targets of cyberattacks. According to a report by the Forward-Looking Threat Research Team, the number of online banking malware detections in India, Brazil and China accounted for 15% of global total in the third quarter of 2015.[1] The second is rampant cybercrime. The US Symantec's 2016 Internet Security Threat Report warned that emerging economies have high rates of cybercrime.[2] The McAfee security firm found that cybercrime's greatest victims are found in the emerging BRICS economies of Russia (85%), China (77%), and South Africa (73%), precisely where connectivity is high but cybercrime security and awareness is low.[3] The third is the common challenge of cyber terrorism. The Global Terrorism Index 2016 released by the London Institute for Economics and Peace indicated that BRICS are threatened by cyber terrorism, with the terrorism index of India, China and Russia ranking the world's 8th, 23rd and 30th respectively.[4] The Fortaleza Declaration issued at the end of 2014 BRICS summit expressed concern at "the increasing use … by terrorists and their supporters, of information and communications technologies (ICTs), in particular the Internet and other media."[5] The Goa Declaration adopted by the 2016 BRICS summit called upon all nations to take a comprehensive approach in "countering misuse of the Internet including social media by terror entities through misuse of the latest Information and Communication Technologies (ICTs)"[6]

Eliminating the digital divide

The "digital divide" refers to the gap between "digital poor" and

---

1   Forward-Looking Threat Research Team, "Ascending the Ranks: The Brazilian Cybercriminal Underground in 2015," A TrendLabs Research Paper, 2015, p.12, https://documents.trendmicro.com/assets/wp/wp-ascending-the-ranks.pdf.

2   Symantec, *Internet Security Threat Report*, Vol. 21, April 2016, p.56.

3   "Cyber-Security and the BRICS," The Global Initiative against Transnational Organized Crime, http://globalinitiative.net/programs/cybercrime/cyber-security-and-the-brics.

4   Institute for Economics & Peace, *Global Terrorism Index 2016*, IEP Report 43, November 2016, pp.10-11.

5   "Sixth BRICS Summit – Fortaleza Declaration," Indian Ministry of External Affairs, July 15, 2014, http://mea.gov.in/bilateral-documents.htm?dtl/23635/Sixth+BRICS+Summit++Fortaleza+Declaration.

6   "Goa Declaration at 8th BRICS Summit," Indian Ministry of External Affairs, October 16, 2016, http://www.mea.gov.in/bilateral-documents.htm?dtl/27491/Goa+Declaration+at+8th+BRICS+Summit.

"digital rich" in the information age, which is demonstrated by the gap in internet penetration rates, and the level and depth of the general public having access to information and telecommunications technologies. The World Economic Forum adopted three drivers of environment, readiness and usage for its Networked Readiness Index (NRI) in 2016, where Russia ranked 41st, China 59th, South Africa 65th, Brazil 72nd, and India 91st.[7] The digital divide problem among the BRICS members is striking. According to Internet Live Stats, as of 2016, the total population of BRICS countries was 3.12 billion, the number of internet users in those countries was 1.45 billion, the number of non-users (those without access to the internet) topped 1.66 billion, and the non-users in each BRICS country exceeded 10 million.[8] The 2017 Affordability Report by the Alliance for Affordable Internet showed that high connectivity costs remain one of the biggest obstacles to achieving the universal access pledge.[9] For example, just 1GB of mobile data costs a Chinese 0.7%, a Brazilian 1.97%, a South African 2.48%, and an Indian 3.55% of their average monthly income.[10] Measured by national income, the prices of Microsoft Office in Brazil, Russia and South Africa are 5 to 10 times the prices in the United States and European Union countries.[11] The BRICS countries need to overcome the "digital divide" by giving full play to the potential of digitalization.

Bright prospects for ICT cooperation

The combined population of the BRICS countries is more than 40% of the world's total. With specific advantages in the ITC field, the BRICS countries are both important markets and exporters of ICT products. China
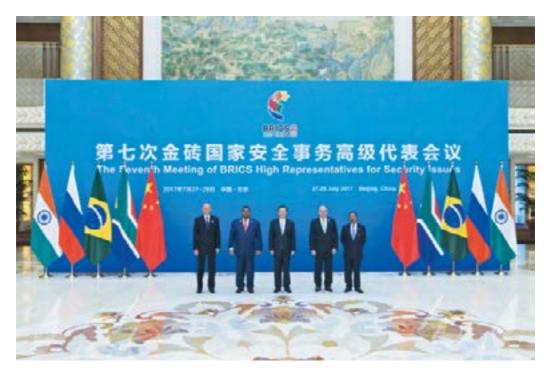
---

7   Silja Baller et al, eds., *The Global Information Technology Report 2016*, Geneva: World Economic Forum, 2016, p.16.

8   Internet Live Stats, *Internet Users by Country (2016)*, July 1, 2016, http://www.internetlivestats.com/internet-users-by-country.

9   Alliance for Affordable Internet, *2017 Affordability Report*, p.6, http://1e8q3q16vyc81g8l3h3md6q5f5e.wpengine.netdna-cdn.com/wp-content/uploads/2017/02/A4AI-2017-Affordability-Report.pdf.

10   Alliance for Affordable Internet, *2017 Affordability Report*, pp.6, 47.

11   Laura DeNardis, *The Global War for Internet Governance*, translated by Qin Qingling, et al., Renmin University Press, 2017, p.201.

Chinese State Councilor Yang Jiechi and high representatives for security issues from Russia, South Africa, India and Brazil attend the seventh meeting of BRICS High Representatives for Security Issues in Beijing, July 28, 2017. The parties agreed to strengthen communication and cooperation in cybersecurity and give play to the roles of meeting and consultation mechanisms at all levels.

is the world's largest exporter of electronic products, with its household electronic appliances occupying over 30% of the world market.[12] Russia takes lead in broadband services among the BRICS countries. The cost of its mobile internet and communications is the second lowest in the world, only higher than Hong Kong.[13] India is a large software exporter, and its information industry is on track to reach the goal of $225 billion in revenue by 2020.[14] South Africa is the leader of Africa's telecommunications industry and its telecom operator is the sponsor of the BRICS Cable. Brazil is a

12 Zhao Yang, "China's Electronic Home Appliances Trade Share Over One-Third of World's Total," *Tencent Digital*, January 19, 2017, http://digi.tech.qq.com/a/20170119/034267.htm.

13 "New Progress in Russia's ICT Industry in 2016," *China Daily*, May 26, 2017, http://world.chinadaily.com.cn/2017-05/26/content_29517360.htm.

14 "Indian Tech Industry Revenue to Touch $350 Billion by 2025: NASSCOM," *Gadgets NDTV*, October 5, 2015, http://gadgets.ndtv.com/others/news/indian-tech-industry-revenue-to-touch-350-billion-by-2025-nasscom-748429.

critical data hub in South America and it has deployed 24 top-class geo-domain mirror servers in its territory.[15]

The BRICS countries have reached consensus on deepening their ICT cooperation. In 2015, the BRICS leaders at the Ufa summit decided to establish a working group on ICT cooperation. In November 2016, the BRICS Ministers of Communications agreed on the common goal of establishing a "digital partnership." Manoj Sinha, India's Minister of Communications, pointed out that the BRICS members have decided to adopt Building Responsive, Inclusive and Collective Solutions (BRICS) in the ICT arena.[16] China Huawei Corporation is actively helping the BRICS countries improve their ICT levels, and has set up communications technology training centers in Russia, India and Brazil. In July 2016, it established Africa's first ICT innovation experience center in South Africa. BRICS countries can benefit most developing countries by exporting electronic products to less-developed countries and sharing the development experience of their information technology industries. China's Huawei Corporation is assisting the other BRICS countries to enhance their ICT capabilities by setting up ICT training centers in Russia, India and Brazil. In July 2016, it established Africa's first ICT innovation experience center in South Africa. The BRICS countries can bring benefits to other developing countries by exporting electronic products to less-developed countries and sharing their experience in developing information technology industries.

Seeking for more equitable global cyberspace governance

In global cyberspace governance, the BRICS countries "advocate for an open, non-fragmented and secure Internet" and reaffirm that "States should

---

15   Shen Yi, "Global Cyberspace Governance and BRICS Cooperation," *International Review*, Issue 4, 2014, p.153.
16   "BRICS Draws Action Plan for Cooperation in ICT Arena," *News Track India*, November 11, 2016, http://www.newstrackindia.com/newsdetails/2016/11/11/346--BRICS-draws-action-plan-for-cooperation-in-ICT-arena-.html.

participate on an equal footing in its evolution and functioning."[17] Joseph Nye has noted that despite the fact that the world powers are unlikely to dominate cyberspace in the way they dominated the oceans or the airspace in the past, the dispersion of power in cyberspace does not mean equality of power.[18] The United States controls the main channels of the global internet, and it is seeking absolute dominance in cyberspace. The "Prism Project" unveiled by former US National Security Agency employee Edward Snowden showed how wide-ranging and deep the United States' global cyber monitoring can be. Cyberspace governance should not satisfy the strategic appeals of a few countries alone, but should represent the interests of different countries and their domestic actors under a multilateral framework. The BRICS countries stress the United Nation's role in cyberspace governance. They actively participate in the formulation of international rules on behalf of emerging economies and developing countries, with the view of pushing forward global cyberspace governance.

New Achievements in BRICS Cybersecurity Cooperation

The BRICS countries have long been engaged in cybersecurity cooperation. The Snowden incident in 2013 provided an important opportunity to advance cybersecurity cooperation among the BRICS countries, and the cybersecurity issue was listed in the BRICS summit statement the same year for the first time. Subsequent BRICS summit statements have contained more elaborations on the framework of cybersecurity cooperation. So far, the BRICS countries have scored great progress in four aspects.

Addressing common cybersecurity threats

The BRICS countries have reached consensus on dealing with the common threats to cybersecurity. In April 2010, the meeting of high-ranking

---

17   "Goa Declaration at 8th BRICS Summit," Indian Ministry of External Affairs, October 16, 2016.
18   Joseph Nye, *Cyber Power*, Cambridge, MA: Belfer Center for Science and International Affairs, 2010, pp.1, 19.

BRIC[19] security officials determined to join hands to combat cybercrime, demanding that "efforts to establish an international mechanism to prevent cyber threats should not neglect the interests of the BRIC and developing countries."[20] In January 2013, Secretary of the Russian Security Council Nikolai Patrushev expounded the consensus reached at a meeting of high-ranking BRICS security officials: first, protecting cyberspace from becoming a platform for terrorists to recruit members and disseminate radical ideologies; second, in combating cyber terrorism and cybercrimes, not only the assailants, but more importantly the organizers, should be sanctioned; third, advancing international cooperation through multilateral mechanisms under the UN framework.[21]

In the wake of the Snowden incident, the BRICS countries in their Fortaleza Declaration "strongly condemn acts of mass electronic surveillance and data collection of individuals all over the world."[22] The joint statement by BRICS foreign ministers on March 24, 2014 further noted that for the "significant infringements of privacy and related rights in the wake of the cyber threats experienced," "there is a need to address these implications in respect of national laws as well as in terms of international law."[23] In September 2016, BRICS high representatives for security issues agreed to enhance cybersecurity by joint efforts, including sharing of information and best practices combating cybercrimes, improving cooperation between technical and law enforcement agencies, and joint cybersecurity R&D and capacity building.[24] Specifically, South Africa has engaged in cooperation with the other four BRICS countries on strengthening capabilities against

19   South Africa, after whose entry BRIC was renamed BRICS, was not a full member of the group at that time.
20   "BRIC Countries to Combat Cybercrime," *Huanqiu*, April 16, 2010, http://world.huanqiu.com/roll/2010-04/781746.html.
21   "BRICS to Counter Cyber Terrorism," *Sputnik News*, January 14, 2013, https://sputniknews.com/voiceofrussia/2013_01_14/BRICS-to-counter-cyber-terrorism.
22   "Sixth BRICS Summit – Fortaleza Declaration," Indian Ministry of External Affairs, July 15, 2014.
23   "Chairperson's Statement on the BRICS Foreign Ministers Meeting Held on 24 March 2014 in The Hague, Netherlands," http://www.dirco.gov.za/docs/2014/brics0324.html.
24   "BRICS Security Advisers Agree to Enhance Cyber Security," *Sputnik News*, September 16, 2016, https://sputniknews.com/world/201609161045368613-brics-cyber-security.

cyber threats, and is actively participating in training programs of other countries.[25]

Developing information infrastructure

In terms of developing information infrastructure, the BRICS Cable is the common strategic investment project of the BRICS countries. The 34,000-kilometer-long project was formally approved at the BRICS Durban summit in 2013 and started in early 2014.[26] The completion of the project will change the situation that each BRICS country is connected by cable hubs located in the US or European countries, reducing the telecommunications cost by 40%. The cable will interconnect with SEACOM, the Eastern Africa Submarine Cable System (EASSy) and the West Africa Cable System (WACS), linking internet infrastructure of the BRICS nations to the rest of Africa.[27] Andrew Mthembu, initiator of the BRICS Cable, noted: "Previously, a call from Johannesburg into Angola would be routed to Pretoria and switched to Cape Town where there is an international satellite gateway. It would then be switched to Belgacom in Europe, who then switch it to satellite and finally to Angola … a direct link will significantly lower the cost of connectivity."[28] Once the Cable is completed, South Africa's interconnection capabilities would allow the BRICS immediate access to 21 other African countries. In this way, a BRICS cable system would essentially open up communications among half of the world's population.[29]

---

25   "SA Struggling to Tackle Cybercrime: Expert," *SABC News*, October 14, 2015, http://www.sabc.co.za/news/a/dcc49f004a33cef2b768ffa53d9712f0/SA-struggling-to-tackle-cybercrime:-Expert-20151014.

26   "Shantou Becomes Landing Place in China for BRICS Cable," *Shenzhen Special Zone Daily*, April 4, 2013, p.A7

27   Stacia Lee, "International Reactions to U.S. Cybersecurity Policy: the BRICS Undersea Cable," Henry M. Jackson School of International Studies, University of Washington, January 8, 2016, https://jsis.washington.edu/news/reactions-u-s-cybersecurity-policy-bric-undersea-cable.

28   James Barton, "South Africa: the Keystone in the BRICS Cable System," *Developing Telecoms*, May 2, 2012, https://www.developingtelecoms.com/tech/optical-fixed-networks/3885-south-africa-the-keystone-in-the-brics-cable-system.html.

29   *Ibid*.

Promoting institutionalized cybersecurity cooperation

The BRICS countries have set up several cybersecurity cooperation mechanisms that constitute an institutionalized cooperative platform to jointly cope with cybersecurity threats. Cybersecurity has become an important issue in BRICS summits, BRICS foreign ministers' meetings and meetings of high representatives for security issues. At a meeting in South Africa's Cape Town in December 2013, the BRICS high representatives for security issues agreed on the establishment of an expert working group on cybersecurity to follow new developments in the field and accelerate mutual consultation and exchanges.[30] In May 2015, they further agreed to prepare "common approaches to information security," informed by a reformed system of global governance that promotes "cooperative, equal, and indivisible security."[31] In July the same year, the seventh BRICS summit decided to establish the meeting mechanism for telecommunications, set up the Working Group of Experts of the BRICS States on security in the use of ICTs to promote sharing of information and best practices relating to security in the use of ICTs, effective coordination against cybercrime, and the establishment of nodal points in member states, etc.[32] The BRICS countries have also set up a mechanism for inputs from think tanks to consolidate cybersecurity cooperation. The BRICS Think Tanks Council (BTTC), which was established in 2013, has been active in providing intellectual support for BRICS cooperation. In January 2017, the China Council for the BRICS Think Tank Cooperation (CCBTC) was established. It convened in May a symposium on cyber-economy and cybersecurity attended by relevant experts from the BRICS states, and provided written proposals for the BRICS Xiamen summit in September the same year. In June 2017, the BRICS

---

30 "BRICS Announce Joint Cybersecurity Group," *The BRICS Post*, December 7, 2013, http://thebricspost.com/brics-announce-joint-cyber-group/#.WMpHcPkQjdI.

31 Tim Stevens, "BRICS Set out Vision for International Information Security", *The Sigers*, July 1, 2015, http://thesigers.com/analysis/2015/7/3/brics-set-out-vision-for-international-information-security.

32 "VII BRICS Summit Ufa Declaration," Indian Ministry of External Affairs, July 9, 2015 http://www.mea.gov.in/Uploads/PublicationDocs/25448_Declaration_eng.pdf.

Political Parties, Think-Tanks, and Civil Society Forum adopted the "Fuzhou Initiative," offering suggestions for deepening cybersecurity cooperation.

Jointly putting forward propositions on cyberspace governance

The BRICS countries have been seeking the right to equal participation in cyberspace governance and standing on behalf of developing countries. In January 2013, the BRICS high representatives for security issues made a statement proposing the establishment of a new global mechanism to block terrorists from inciting large-scale turmoil in cyberspace and spreading false information. Then India's National Security Advisor Shivshankar Menon noted at the meeting that cybersecurity is an issue of common concern.[33] In April 2013, the BRICS countries submitted to the United Nations, in the name of BRICS for the first time, a draft resolution entitled "Strengthening International Cooperation to Combat Cybercrime," demanding that the UN accelerate the study and response to cybercrimes. This is the first time the BRICS countries issued a joint initiative on cybersecurity. The Goa Declaration at the eighth BRICS summit in October 2016 highlighted that the BRICS countries would "work together for the adoption of the rules, norms and principles of responsible behavior of States including through the process of the United Nations Group of Governmental Experts (UNGGE)."[34]

Challenges for BRICS Cybersecurity Cooperation

Although the rise of BRICS countries has, as a whole, challenged the hegemony of the United States in global cyberspace, they still face three major challenges in their cybersecurity cooperation, namely different conceptions of cyberspace governance, internal constraints of cybersecurity

---

33   "Terrorism, Cyber Security Issues Dominate BRICS Security Meet," *Daily News Analysis* January 10, 2013, http://www.dnaindia.com/india/report-terrorism-cyber-security-issues-dominate-brics-security-meet-1787706.

34   "Goa Declaration at 8th BRICS Summit," Indian Ministry of External Affairs, October 16, 2016.

cooperation and differentiation policies of Western countries.

Different conceptions of cyberspace governance

The BRICS countries are actively involved in global cyberspace governance and are striving for rules-making power, but they can be divided into two groups on the issue of cyberspace governance. One group is represented by China and Russia, who attach importance to the state's control over the cyberspace and pay attention to the threat of using computer technologies to undermine national sovereignty and security or interfere in internal affairs. On May 8, 2015, China and Russia signed an agreement on cooperation in ensuring international information security and reached a consensus on applying the principle of national sovereignty to cyberspace. Both countries promised not to conduct hacker attacks on each other. In October the same year, China and Russia conducted the "Xiamen 2015" anti-cyber terrorism drill under the framework of the Shanghai Cooperation Organization. The other group, represented by India, Brazil and South Africa, focuses on building a people-centered, inclusive and development-oriented information society and is committed to deepening cooperation in building such an information society. In September 2006, the India-Brazil-South Africa (IBSA) Dialogue Forum signed the Framework Agreement for Cooperation on the Information Society. In October 2011, the three countries issued the Tshwane Declaration, recommending the establishment of an IBSA Internet Governance and Development Observatory that would be tasked to monitor developments in global internet governance and provide regular updates and analyses from the perspective of developing countries.[35] Western scholars mark

To promote cybersecurity cooperation under the BRICS framework, China and Russia need to gain the support of the other three countries for their cyberspace governance initiative.

---

35   "Fifth IBSA Dialogue Forum - Tshwane Declaration," Indian Ministry of External Affairs, October 18, 2011, http://www.mea.gov.in/bilateral-documents.htm?dtl/5321.

India, Brazil and South Africa as the "swing states" in global cyberspace governance. They are characterized by pro-activeness, but are careful not to align with either the United States or Sino-Russian initiatives.[36] To promote cybersecurity cooperation under the BRICS framework, China and Russia need to gain the support of the other three countries for their cyberspace governance initiative.

Internal constraints facing BRICS countries

Some BRICS countries hold negative positions on cybersecurity cooperation due to their own national interests and domestic pressure, which makes it difficult to make breakthroughs in substantive cooperation under the BRICS framework. During the Ufa summit in 2015, India raised objections to the agenda of cyberspace governance and e-commerce cooperation, resulting in the failure of reaching a consensus. Russia, as the host country of the Ufa summit, took international information security as the focus of cooperation and proposed to make BRICS "a collective leader in the global community on strengthening international information security."[37] While Moscow circulated a draft among BRICS members that devoted substantial space to internet governance ahead of the summit,[38] India announced at the summit its desire to move from state-led internet governance to a more multi-stakeholder perspective, which made Russia strongly dissatisfied.[39] In terms of e-commerce cooperation, Indian Minister of Commerce and Industry Nirmala Sitharaman also expressed opposition to advancing cooperation in this area at a BRICS Expert Group meeting in June the same year. "Russia and China are pushing for an agreement

---

36   Hannes Ebert and Tim Maurer, "Contested Cyberspace and Rising Powers," *Third World Quarterly*, Vol.34, No.6, 2013, pp.1054-1074; Hannes Ebert and Tim Maurer, "Cyberspace and the Rise of BRICS," *Journal of International Affairs*, July 2013, https://jia.sipa.columbia.edu/online-articles/cyberspace-and-rise-brics#_ftnref14.

37   "Concept of the Russian Federation's Presidency in BRICS in 2015-2016," Official Website of Russia's Presidency in BRICS, March 1, 2015, http://en.brics2015.ru/russia_and_brics/20150301/19483.html.

38   Arun Mohan Sukumar, "A BRICS Vision for the Internet," *The Hindu*, July 9, 2015, http://www.thehindu.com/opinion/op-ed/brics-leaders-meet-in-ufa-for-the-annual-summit/article7400020.ece.

39   Stacia Lee, "International Reactions to U.S. Cybersecurity Policy: the BRICS Undersea Cable".

on cross-border trade through e-commerce. We are slightly defensive on the e-commerce agenda at BRICS. The main reason is that our domestic policies on e-commerce are still evolving," an Indian government official said.[40] In response to an agreement signed with China in information and communications technology in June 2015, South Africa's opposition party Democratic Alliance expressed dissatisfaction, saying that no issue of cybersecurity or internet governance should be solely in the domain of the government but should represent "the interests of multi-stakeholders."[41]

Differentiation policies of Western countries

Over the ten years of BRICS development, Western countries have been adopting a differentiation policy and raising various pessimistic arguments against the group, such as the collapse of BRICS, the fading influence of BRICS or the dissolution of BRICS. Nikolai Patrushev pointed out that the West has increasingly been using international financial institutions as an instrument of pressure. The overall capital outflows from the BRICS economies have amounted to at least $3.5 trillion over the past ten years, with outflows in the past three years accounting for over half of this.[42] It was pointed out that the United States actively carried out "soft coups" in Brazil and South Africa and fostered pro-American factions in the two countries to seek a regime change, with a strategic intention to internally disintegrate the BRICS.[43] The US has also continuously deepened its cooperation and dialogue with India in cybersecurity and hopes India will accept the US-led cybersecurity order. Alex Grigsby, a scholar at the US Council on Foreign Relations, pointed out that for years the US has been courting both India

---

40   "India May Oppose BRICS Proposal for Cooperation in E-Commerce," *Live Mint*, June 24, 2015, http://www.livemint.com/Politics/zuT2OUbIAWawSYsdO1vtKL/India-may-oppose-Brics-proposal-for-cooperation-in-ecommerc.html.
41   Gareth van Zyl, "SA-China Cyber Security Pact Worries DA," *Fin24 Tech*, June 10, 2015. http://www.fin24.com/Tech/News/SA-China-cyber-security-pact-worries-DA-20150610.
42   "The West Has Sucked $3.5 Trillion out of BRICS over 10 Years," *Russia Insider*, May 29, 2015, http://russia-insider.com/en/politics/west-has-sucked-35-trillion-out-brics-over-10-years-top-russian-spy/ri7558.
43   Hugo Turner, "'Soft' Coups Threaten Brazil, Venezuela and South Africa," *Global Research*, May 14, 2016, http://www.globalresearch.ca/soft-coups-threaten-brazil-venezuela-south-africa/5525142?print=1.

and Brazil to promote its preferred norms for cyberspace, hoping that the two countries will bandwagon in support of the US vision of an open, global, free and resilient cyberspace.[44] If the BRICS countries want to represent the interests of developing countries, they should strengthen their internal cooperation instead of totally accepting the cybersecurity initiatives of the US.

Paths to Deepen BRICS Cybersecurity Cooperation

The BRICS countries have the common strategic intention to reform the global cyberspace governance system. They have reached consensus on the common cybersecurity threats and measures in response to these threats, and have built some cooperative mechanisms. The BRICS countries can develop their cybersecurity cooperation agenda in the following four aspects.

Perfecting cooperation platform to counter cyber threats

The BRICS countries should perfect their cybersecurity cooperation platform to fight against cybercrimes and cyber terrorism. To succeed in jointly cracking down on grave cybercrimes, the BRICS countries must integrate well the existing mechanisms, and enhance exchanges and coordination of the Meeting of Cybersecurity Working Group, the Meeting of the Heads of Customs Administration, the Meeting of the Heads of Prosecution Services, and the Justices Forum, in an effort to bolster law enforcement cooperation in cybersecurity. In view of emerging cyber threats such as ransomware and cyber terrorism, BRICS can establish a permanent cyber threat observation, early warning and response mechanism, monitoring the cybersecurity situation in BRICS countries, issuing early-warning reports timely, and protecting critical information infrastructure such as energy and electricity in member countries from being spoiled. The members of BRICS can set up BRICS Cybersecurity Centers comprising

---

44   Alex Grigsby, "Do India and Brazil Really Moderate China and Russia's Approach to Cyberspace Policy?" Council on Foreign Relations, April 26, 2016, https://www.cfr.org/blog-post/do-india-and-brazil-really-moderate-china-and-russias-approach-cyberspace-policy.

technical experts and appoint BRICS Cyber Coordinators, to maintain the order of cyberspace.

Boosting intergovernmental cooperation through civil dialogues

The private sector and civil society are important participants in cyberspace governance. In areas where intergovernmental cooperation is unable to achieve breakthroughs, high-tech companies or think tanks can hold roundtable meetings to address the concerns of member countries through informal consultations and explore constructive paths to boost official cooperation. Russian cybersecurity expert Oleg Demidov said that the tech community and private sector in the BRICS countries can help bridge gaps between the official positions of the five countries' governments on all key issues concerning internet governance.[45] In 2017, a symposium was held by think tanks of BRICS countries on digital economy and cybersecurity, suggesting that think tanks provide intellectual support for cybersecurity cooperation. The BRICS countries can also make in-depth exchanges on smart city and smart social initiatives, and foster new areas of economic cooperation.

If the BRICS countries want to represent the interests of developing countries, they should strengthen their internal cooperation instead of totally accepting the cybersecurity initiatives of the US.

Pioneering information technological cooperation

Compared with developed countries, the BRICS countries have unique advantages in propelling information infrastructure building and technological advance, and they are supposed to make the BRICS mechanism the pioneer of information technological cooperation between developing countries. In terms of information infrastructure, in January 2016, KPMG International published a report "Foresight: A Global

---

45 "BRICS and the Internet." Official Website of Russia's Presidency in BRICS, April 10, 2015, http://en.brics2015.ru/news/20150410/40202.html.

Infrastructure Perspective" that listed ten emerging trends that would change the world of infrastructure over the next five years. It stated that the center of gravity of the global infrastructure market has moved to the East, and China and India have left the Western countries behind in this field.[46] The BRICS countries can break the monopoly of developed countries on core cyber technologies by laying fiber optic cables, providing digital products and services and sharing R&D experience, eliminate the digital divide that confronts developing countries, and make more people in developing countries benefit from the opportunities brought by the internet. The BRICS countries can also raise the cybersecurity levels in developing countries by organizing cybersecurity technology training courses.

Advancing formulation of global cyberspace rules

The BRICS countries can accelerate the formulation of global cyberspace rules in three aspects. First, by maintaining the United Nation's core role in global cyberspace governance, the BRICS can publish its proposals for cyberspace governance, and advance the transformation in global cyberspace governance under the UN framework. Second, the BRICS can seek for establishment of international norms that guarantee the participation in cyberspace by all countries on equal terms, and oppose infringement of cyber sovereignty or attacks on critical information infrastructure of other countries. Third, the BRICS can put forward policy initiatives on cyber sovereignty, fighting cybercrimes, and countering cyber terrorism, and raise cyber governance programs that take into account both state control and social participation and meet the interests of developing countries. The BRICS countries need to gather consensus and contribute their efforts and wisdom to building a new order of global cyberspace governance.

---

46   KPMG, "10 Emerging Trends in 2016," *Foresight*, January 2016, https://assets.kpmg.com/content/dam/kpmg/pdf/2016/05/11702Emerging-Trends-v2-web.pdf.