Dr. Vladimir A. Orlov[1]

New Threats and Challenges to Global Security: A View from Russia

BRICS 2016 Academic Forum

Goa, India

September 19-21, 2016

When the leaders of our five nations met in July 2015 in Ufa, they agreed "to step up coordinated efforts in responding to emerging challenges, ensuring peace and security" through further enhancement of "our strategic partnership on the basis of principles of openness, solidarity, equality and mutual understanding, inclusiveness and mutually beneficial cooperation"[2].

In this context, leaders of the BRICS nations expressed their support "for international efforts to address these challenges in a way that provides equal and indivisible security for all states, through respect for international law and principles of the UN Charter"[3].

Indeed, addressing multiple new threats and challenges to the global security architecture in a cooperative, well-coordinated and result-oriented way is a huge task for the BRICS "Peace and Security" basket by itself.

While in certain areas the progress is visible, there is a lot more to be done to improve the level of coordination in order to achieve tangible results that would be mutually beneficial and satisfactory.

I would concentrate on five areas, both in 'hard' and in 'soft' security[4], where such progress in both desirable and, in my view, achievable as BRICS' positions on these areas, although not identical, are rather close, and resolving them would meet the national interests of each of our nations.

I. Fighting against the terrorism of use of weapons of mass destruction (WMD)

In the Ufa Declaration, the BRICS leaders reiterated their "strong condemnation of terrorism in all its forms and manifestations" and stressed that "there can be no justification, whatsoever, for any acts of terrorism, whether based upon ideological,

---

[1] Dr. Vladimir A. Orlov is a member of the National Committee for BRICS Research. He is the Head of the Center for Global Trends and International Organizations at the Diplomatic Academy of the Ministry of Foreign Affairs of the Russian Federation; and Founder & Special Advisor to the Moscow-based PIR Center. He can be reached at orlov@pircenter.org

[2] Seventh BRICS Summit. Ufa Declaration. July 9, 2015.

[3] Ibid.

[4] I would like to thank my colleagues at PIR Center Gen. Yevgeny Buzhinsky, Mr. Oleg Demidov, Mr. Andrey Baklitsky, Mr. Albert Zulkharneev, and Ms. Natalya Kosolapova for their ideas and contributions to this analysis.

religious, political, racial, ethnic, or any other justification". They expressed their determination to consistently strengthen our cooperation in preventing and countering international terrorism, with the understanding that "the UN has a central role in coordinating international action against terrorism". They believed that "terrorist threats can be effectively addressed through a comprehensive implementation by states and the international community of all their commitments and obligations arising from all relevant resolutions of the UN Security Council and the UN Global Counter-Terrorism Strategy"[5].

I would like to remind that already two years ago, in 2014, the BRICS Think Tank Council (BTTC) created a road map "Towards a long-term strategy for BRICS". It proposed, inter alia, that BRICS should strengthen cooperation between relevant law enforcement agencies to exchange information and provide mutual assistance in the pursuit of criminals fleeing prosecution for terrorist activities, and establish a joint monitoring system over those suspected of involvement in terrorist activities. It might be deemed necessary for BRICS to provide ad hoc cooperation on joint investigation of terrorist activities in BRICS countries, with a commitment to extradite terrorists plotting or implementing terrorist acts in any of the BRICS countries.

WMD terrorism is the most dangerous, and potentially most disastrous, form of terrorism. Nuclear materials and munitions, chemical agents or biological weapons in the hands of terrorists, whether in the Middle East, in South Asia, East Asia, North Africa, or in any other region of the globe could make nightmare scenarios reality.

Syria was, until recently, one of the cases where the terrorists were making attempts to use chemical weapons blaming the government of Syria for their use[6]. In this regard, I find of importance the Ufa Declaration statement condemning "any use of toxic chemicals as a weapon in Syria. We commend the outcome of setting international control over the Syrian arsenals of chemical weapons and transferring toxic substances and their precursors from Syrian territory"[7].

The crisis with the chemical weapons in Syria and with the danger of terrorists getting access to them was resolved thanks to the efforts of the Russian Federation, other major players, as well as the Syrian government who agreed to dismantle its own CW arsenal under international control and to join the Chemical Weapons Convention (CWC).

At the same time, this situation demonstrated the urgency of addressing the issue of chemical, as well as biological, weapons if they fall in the hands of violent non-state actors. According to studies by PIR Center, *the Poor Man's Nuclear Weapons* appeal increasingly to the most aggressive international terrorist organizations. At the same time, unlike the situation with the nuclear weapons where there is a UN Convention

[5] Ibid.

[6] On 8 March 2015, the Kurdish People's Protection Units claimed that terrorists, including from Ahrar al-Sham, used what is presumed to have been phosphorus munitions in an attack on an area in Aleppo. In June 2015, terrorists used "improvised chemical munitions" to attack Kurdish rebels in the Al-Hasakah Province in northeast Syria. Later, the use of chemical weapons by "Islamic State" against the Syrian Kurds was confirmed by an investigation conducted by two independent research organizations based in the United Kingdom. Accidents in the Syrian town of Marea in August-September 2015 where, as the OPCW mission has established, the ISIL militants used artillery shells filled with sophisticated chemical warfare agent – Sulphur mustard – testify to the extreme urgency of the situation.

[7] *VII BRICS Summit, Ufa Declaration*, National Committee for BRICS Study, Russia, July 9, 2015.

Against the Acts of Nuclear Terrorism, there are no norms in international law concerning CW or BW.

On March 1, 2016, Russia's Foreign Minister Sergey Lavrov proposed to develop (within the framework of the Conference on Disarmament in Geneva) Convention on the Suppression of Acts of Chemical Terrorism: "The threat of WMD falling into the hands of non-state actors is a generally recognized. A lot has been done to counter this threat. The adoption of the UNSC resolution 1540 back in 2004 was an important step in this direction. The International Convention for the Suppression of Acts of Nuclear Terrorism was concluded on the Russian initiative a year later. However, we still face significant gaps related, in particular, to the use of chemicals for terrorist purposes. Nowadays this threat is getting extremely urgent in the light of newly revealed facts of repeated use of not only industrial toxic chemicals but also of full-fledged chemical warfare agents by the ISIL and other terrorist groups in Syria and Iraq. There is a growing jeopardy of similar crimes in the territory of Libya and Yemen as well" [8].

Russian experts have analyzed reports on terrorist groups getting access to scientific and technical documentation on the production of chemical weapons, seizing plants with relevant equipment and engaging foreign specialists to help synthesize chemical warfare agents[9]. It does not leave any doubt that chemical terrorism is emerging not as an abstract threat, but a grave reality of our time which could and should be addressed through intensified meaningful work in international fora.

It should be taken into consideration that the CWC does not fully address the challenge of countering chemical terrorism. Also, we do not see grounds for statements on the sufficiency of the already existent of norms of the customary international law. These norms do not solve the task of prohibiting the use of chemical weapons by non-state actors and even qualifying such actions as an international crime. We can hardly expect to bridge these gaps by developing amendments to the CWC, as it lays down an overly complex and time-consuming procedure for the amendments adoption.

It seems that a more realistic, reliable and promising way of tackling this problem is o elaborate a stand-alone convention for the suppression of acts of chemical terrorism. Yet, we propose to embark on this task here, in the Conference on Disarmament, which has already made an invaluable contribution to the reduction of the chemical weapons threat through successful elaboration of the CWC.

Later this year, the WMD terrorism-related issues were raised at the Vth Moscow Conference on International Security. Russia's initiative was further elaborated by China. A Chinese delegate to the conference, Mr. Chang Wanquan, highlighted the danger of the growing threat of nuclear terrorism.[10] Further on, Russia and China reformulated the Russian proposal at the CD, adding biological weapons terrorism to the chemical weapons terrorism, so that the proposed convention should address both.

[8] Statement by Mr. S. Lavrov to the Conference on Disarmament, document CD\PV.1379, March 1, 2016.

[9] Vladimir Orlov, Terrorism and "Poor Man's Nuclear Weapons", *PIR Center Blog of Vladimir Orlo*v (July 26, 2016), < http://pircenter.org/en/blog/view/id/260>, last accessed September 13, 2016.

[10] Chang Wanquan, Speech on the Conference, paper delivered to Vth Moscow Conference on International Security, sponsored by the Ministry of Defence of the Russian Federation, April 27-28, 2016.

Experts have noticed a generally positive reaction to the Russian proposal by India, and no objections in principle by other BRICS nations.

Unfortunately, however, there has been no progress in Geneva on the Conference on Disarmament in relation to this issue so far.

BRICS nations, in my view, should find mutually acceptable, beneficial, and creative ways to address the international legal implications of the chemical and biological terrorism while at the same time saving the Conference of Disarmament itself from collapsing.

While the risk of nuclear terrorism is concerned, it is essential for all nations with nuclear installations, including all BRICS countries, to work hard on improvement of nuclear security. In this context, I would like to draw attention to a recent report prepared by PIR Center and entitled "Assessing the State of Nuclear Security at the National Level". The report has provided a new methodology for assessing the state of nuclear security at the national level, and has invited to apply that methodology to a group of countries on a trial basis.

Given the range and gravity of the existing threats, nuclear security must be regarded as the top priority for the international community. Countries with established nuclear programs (like all of the BRICS countries) could do more to ensure that the states which start their nuclear path had the best available protection for their nuclear facilities and materials. In order to do so those countries should:

1. Further support the IAEA in its assistance to the nuclear newcomer countries by providing necessary funds as well as the technical expertise and creative ideas (like advising the Agency to increase the scope of the IAEA's International Physical Protection Advisory Service (IPPAS) to cover nuclear material control and accounting).
2. When acting as nuclear exporters they could make the provision of assistance to improve the state of nuclear security in the importer countries part of the agreements and contracts they sign with these countries.
3. Encourage nuclear newcomers to refer to the IAEA for expertise and evaluation (including IPPAS missions) and implement the recommendations provided by the Agency.

II. ICT and Cyber Security

Today the BRICS states constitute one of the most massive and rapidly growing segments of the global Internet community. In 2016 total number of Internet users in BRICS states exceeds 1,45 billion (which accounts for 42 per cent of the world's Internet audience). In China and India share of the internet economy in the GDP is higher than the developed market average and both countries are in the world top-5 by this factor[11].

Nevertheless, the BRICS still was not able to consolidate and articulate the voice of the non-Western world and the developing countries on vital issues related to the ICTs in

[11] Oleg Demidov, "BRICS: Synergy Potential for Global Internet Governance and Cybersecurity Agenda", eds., *Global Internet Governance and International Security in the Field of ICT Use* (PIR PRESS, 2016), 88 p.

international security and global governance field. Neither the global discussion on transition of the oversight of the critical Internet functions, kick-started by the USG statement from March 14, 2014, nor the attempt to set global rules to stop uncontrolled governmental surveillance in the Internet which emerged and failed at the NETMundial summit in April 2014, did not reveal any consistent and concrete BRICS position on these issues. BRICS countries still prefer to act in their own capacity – like Brazil who hosted the NETMundial summit or China who hosted Wuzhen Summit in the end of the 2015.

In fact, the ICT agenda remains a "missing pillar" in the BRICS identity and agenda, as its elaboration has been limited to trivial passages on the benefits of the global ICT revolution repeated in each BRICS Summit declaration. This situation seems to be a paradox taking into account the immense role of the group's states in the global ICT sector, and their intensive cooperation in other areas, such as reform of the global financial architecture. Though BRICS was initially aimed at reforming existing institutions, primarily economic ones, the association should play a major role in reforming internet governance institutions as well. 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.

What could BRICS states do in order to claim its leadership on crucial ICT issues today?

First, to provide a consensus-based vision of the new global Internet governance architecture. BRICS could formulate a global Set of Principles of the Internet Governance, which could include:
1) limits to governmental e-surveillance and responsibility of states for conducting it;
2) the right for access to the Internet;
3) globalization of the Internet governance, implying responsible international control over the Internet's critical functions
The document could also encompass already existing and widely accepted basic principles like the multi-stakeholder approach, network neutrality, openness, integrity, universality of the Internet, etc.

The draft Set of Principles of Global Internet Governance might be promoted in the form of the UN convention or an international treaty that would not fix any liabilities of particular Parties, but would rather postulate the universal principles of cooperation.

Second, elaboration and promotion of "confidence matrix" in the field of the use of ICTS might be a strategically wise move. Russia and China, as members of Shanghai Cooperation Organization, in 2015 presented to the United Nations a draft International Code of Conduct for Information Security. Other BRICS countries could support and develop this initiative. A technical, unpoliticized object provides the better the chances to come to agreement. In addition to sharing information on major abnormalities of trans border traffic and cybersecurity incidents, states could join their forces for monitoring cyber espionage and e-surveillance campaigns targeted at their territory and infrastructure by third parties. The next step could include enabling greater openness of their own trans border flow for their partners in the forum in order to show that they do not conduct cyber espionage or surveillance activities themselves. Another example of productive technical cooperation that would not be controversial is leveraging

cooperation of CERTs (or creating BRICS-CERT or BRICS-CSIRT), which also helps to counter trans border cybercrime and cyber terrorism.

BRICS needs to come to a common understanding on cyber security. This is important given the growing online populations as well as the rise of digital commerce in these countries. In fact, 38% of the global internet audience is from the BRICS countries. Given their large online populations, India, Brazil, and China are considered to be "swing states" in the discourse on cyberspace and cyber security. However, BRICS are underrepresented in the field of global internet governance and cyber governance. Moreover, most of the discourse on management of cyber-space currently emanates from the West. In fact, the BRICS Foreign Ministers' meeting on the side lines of the UNGA in 2013 had expressed concern about "unauthorized interception of communications and data from citizens, businesses, and members of governments, compromising national sovereignty and individual rights". They reiterated the need to participate and contribute "in a peaceful, secure, and open cyberspace" and emphasized the importance of "security in the use of Information and Communication Technologies (ICTs) through universally accepted norms, standards, and practices".

BRICS could exchange best practices in fighting cyber-crime and have regular institutionalized meetings of their emergency response teams. They could establish a working group on cyber security, inform each other of cyber-crimes, and share experiences about fighting cyber-crime. At Fortaleza, BRICS recommitted to the negotiation of a universal legally binding instrument in cybercrime while reiterating that the UN has a central role in this matter. It is also critical that the BRICS countries come to a common understanding on cyberspace governance and cyber security. They need to come to a middle path on the crucial issue of freedom of expression versus legitimate security interests of states. It is heartening that the NSAs have already discussed cooperation in this arena in their meetings.

III. Cyber Security of Civil Nuclear Facilities

Two topics addressed above – WMD terrorism and cyber security – overlap when it comes to the issue of cyber security of nuclear facilities, both military and civilian. While military nuclear facilities should not be covered by any international efforts and should remain issues of national security for each of those BRICS nations to whom this is applicable, civil nuclear infrastructure vulnerabilities should become an issue of our collective attention, as all five BRICS countries have and develop their civilian nuclear programs.

Country	Number of Reactors		Electricity Production Share in 2015
	Operational	Under construction	
Brazil	2	1	2,76 %
China	36	20	3,03 %
India	22	5	3,53 %
Russia	36	7	18,59 %
South Africa	2	0	4,73 %

**Source*: IAEA PRIS[12]

In July 2016, the UN Secretary-General's report on the work of his Advisory Board on Disarmament Matters identified the threat of cyber attacks by terrorists on nuclear facilities as one of the two "most serious threats" (the other being the potential role of cyber in threatening bio-security)[13].

In a report, produced earlier this year by PIR Center in partnership with the World Economic Forum (WEF) and the Centre russe d'etudes politiques (Switzerland), authors came to the conclusion that operators of critical infrastructures all over the world are facing increasing cyber risks[14].

The danger is coming not from accidental software and hardware failures or human factor as it used to be. The threat focus is shifting towards purposeful cyber-attacks on critical facilities, conducted by skillful actors with both criminal and policy motivation. The bad news is that fundamental technology trends play to greater vulnerability of their IT infrastructures. Critical infrastructures become increasingly connected – an inevitable trend dictated by optimization of business processes. Its dark side is a front door of critical facilities open wide for cyber intruders. Among all critical sectors, there is a particularly bright illustration for these trends – peaceful nuclear installations, a new target No.1 for advanced actors in cyberspace.

Civil nuclear installations in a number of countries already became targets for malicious cyber activities. Prominent cases include worm infection of the David-Besse NPP in 2003, Stuxnet (Iran) and the Olympic Games operation in 2005-2012, cyber-espionage campaign against KHNP power plant operator in December 2014, and worm infection of the Gundremmingen power plant in Germany in April 2016. The list is to be continued, as basic observations from those incidents prove:

- Damage threshold for targeted assets has drastically increased. State-of-the-art cyber weapons directly target field devices and are designed for full-scale cyber sabotage operations. A notorious example is Stuxnet.
- Revealing and investigating the incident might not be enough to displace the threat, because attackers' tools are easily modified and re-used.
- Threat vectors drift from traditional ones and include attacks on third parties, social engineering and other innovative techniques.

Several technological trends are changing the way IT infrastructures evolve in the peaceful nuclear energy sector. First, online connectivity now goes beyond corporate and office networks of power plants and enrichment facilities. Field devices that enable operation of critical industrial processes of nuclear facilities are also digitalized and connected online. Another connected segment includes sensors and actuators installed at industrial equipment, monitoring its performance and sending data to parameter

[12] PRIS, IAEA Official Web site, <https://www.iaea.org/PRIS/CountryStatistics/CountryStatisticsLandingPage.aspx>, last accessed: September 13, 2016.

[13] Work of the Advisory Board on Disarmament Matters. Report of the Secretary-General. A/71/176. July 21, 2016.

[14] Cybersecurity of Civil Nuclear Facilities: Assessing the Threat, Mapping the Path Forward. PIR Center. Moscow – Geneva. 2016.

monitoring systems. However smart and convenient, those systems and devices are becoming too numerous and hard to integrate in a secure way. Second, corporate and office segments of nuclear facilities' networks are widely connected to the Internet for a smoother exchange of data with external contractors, consultants, etc. These trends are accompanied with "mobile revolution", growing market of remote online services for managing industrial control systems over the Internet from one's mobile device ("SCADA in your pocket"). These innovations extend the network defense perimeter and create new potential pathways for attackers.

Though these trends take place among all critical infrastructures, peaceful nuclear facilities are a remarkable case. Each nuclear power plant has hundreds of industrial control systems and tens of thousands of detectors and actuators. The consequences follow:

1. Complexity of nuclear installations limits the applicability of previous experience and best practices in terms of ensuring cybersecurity.
2. Huge number of critical IT components make operators depend on too many vendors; besides, it is almost impossible to ensure integrity of supply chains.
3. Standard cybersecurity approaches are not enough. Advanced strategies are needed, such as cybersecurity by design, real-time event management, deployment of cryptography on industrial networks. Those are hard to put in place instantly, without really big longer-term investments and regulatory debates.

Our governments are making some efforts, but are largely dragging behind the evolution of threats. In most countries cybersecurity of nuclear facilities is just emerging as a separate regulatory framework, with a number of issues slowing the process down. Those include ambiguity in division of regulatory agenda between governmental agencies, gaps and overlaps in the regulators' functions.

On the international level, mitigation of cyber-attacks on nuclear installations faces legal vacuum. No international mechanisms aimed at countering and preventing such acts are in place. Sensitiveness and national security considerations make this agenda fall out of the scope of anti-cybercrime frameworks, such as the Convention on Cybercrime adopted by the Council of Europe in 2001. One format which is trying to address cyber protection of critical infrastructures is the United Nations Group of Governmental Experts on cybersecurity. Yet, their proposals to nation states are put as voluntary non-binding norms and do not address nuclear installations directly.

On technical level, new approaches need to be put in place, primarily through collaboration of operators and IT vendors. To eliminate backdoors in critical equipment, penetration- and fuzz testing, deep scanning of programmable field devices firmware is required. More intensive exchange of experience and best practices between leading IT vendors and CNF operators might be helpful. Operators could benefit from adopting cybersecurity by design and deployment of cryptographic tools in their industrial networks. For nuclear power plants, disclosure of the field devices' source code to operators might be a viable option.

Another strategic goal could be deeper integration of cybersecurity into nuclear security paradigm in order to eliminate functional gaps and overlaps between cyber and nuclear regulators. To achieve that, internal dialogue among national regulators should be intensified and promoted by governments and supported with comprehensive

legislation on nuclear cybersecurity. Here, IAEA's role remains instrumental in terms of accumulating best practices from advanced states and providing reference models for developing ones. Governments also have to breed a generation of cybersecurity specialists with a new mindset, able to complement and enhance traditional nuclear security approach. That requires innovations in the higher education system and support of trainings, workshops and dialogues involving both nuclear and IT industries.

Internationally, the UN Group of Governmental Experts' work could be helpful for resolving the taxonomy, terminology and classification of critical nuclear infrastructures and cyber threats to them. Meetings of the 5th Group in 2016-2017 might contribute to shaping shared vision on the issue, if its new report would directly address cyber protection of nuclear installations and contain proposals for non-binding norms. Some of earlier Group's proposals could be updated to address the issue ensuring the integrity of supply chains for critical IT systems procured to nuclear operators.

BRICS could develop general single terminology concerning cyberterrorism, recommendations and standards on nuclear facilities against cyberattacks.

BRICS can be the platform for finding new alternative approaches to global security and cybersecurity in particular.

IV. Non-weaponization of outer space

Over the last decades, peaceful use of outer space (mainly in the low Earth orbit) became indispensable for world economy and global development. Satellites provide communication, imaging, navigation, internet access and much more. BRICS countries invest heavily in the space activities; in 2015, BRICS (mainly Russia, China and India) operated 60% of the world space launches and a healthy percentage of satellites. Unfortunately, this global commodity is poorly regulated and protected, which poses a threat to its efficient use. One of the most ominous scenarios is based on the weaponization of outer space.

Though the Outer Space Treaty (Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and other Celestial Bodies, 27.01.1967) bars states parties to the treaty from placing nuclear weapons or any other weapons of mass destruction in orbit of Earth, installing them on the Moon, or any other celestial body, or otherwise station them in outer space, it does not bar any state from deployment in outer space of any other types of weapons. Under current laws on space, no weapons are prohibited from being deployed in space except for weapons of mass destruction; neither are there any restrictions on the development, testing or deployment of anti-satellite weapons in space.

This opens the door for all sorts of weapons appearing in space, for example laser, kinetic, electro-magnetic, particle-beam weapons. Some countries also possess electronic warfare weapons (high power orbital radio frequency transmitters capable of destroying or incapacitating the electronics of space-based combat control and communication systems, as well as disabling satellites of the adversary's missile warning system).

Deployment of weapons in outer space for BMD and anti-satellite activities will lead to creation of rather numerous orbital groups of space vehicles, flight trajectories of which will be in low orbit area (below 1000 km). These groups may complicate use of this area by other states for various peaceful purposes: for example – distant probing of Earth or piloted space flights. Any space conflict will not only result in loses of satellites but will also produce big amount of space debris that will flood already overcrowded orbit.

The above-mentioned problem has become even more acute after the announcement by the United States of the plans to deploy global system of anti-missile defense, which was followed by the withdrawal of Washington from the ABM Treaty. After the ABM Treaty ceased to exist, the international space law lost one of its key elements – ban on the creation, testing and deployment of anti-missile defense systems and their components in space. Possible appearance of such elements in space may be the first step on the way to turn it in the new sphere of weapons' deployment.

On February 12, 2008, China and Russia jointly submitted a draft of the legally binding Treaty on the Prevention of the Placement of Weapons in Outer Space, the Use of or Threat of Use Force against Outer Space Objects (PPWT) to the Geneva Conference on Disarmament. It was initially introduced to the CD with the "research mandate", which allows for amendments and corrections to the text. Since 2008, a great deal of work was done to coordinate positions on the draft of the treaty, including with the BRICS countries. Brazil and India had reservations against the treaty; they had developed space programs and wanted to make sure that such a treaty would not tie their arms. As the result of those consultations, a new draft treaty was introduced to the CD in July 2014.

The authors of the treaty believe that such a legally binding treaty would prevent the outer space from weaponization.

BRICS position has also evolved over time, the group has supported Russian initiative on 'No First Placement of Arms in Outer Space,' presented at the UN General Assembly. All of the BRICS countries agree that outer space should remain free from any kind of weapons and snit-satellite weapons should be banned. This is in a sharp contrast with the position of the number of countries championed by the United States, which see the outer space as just another domain like land, sea or airspace and thus suitable for different military operations.

With this in mind BRICS Ufa declaration of July 9, 2015 stated that:

1. negotiations for the conclusion of an international agreement or agreements to prevent an arms race in outer space are a priority task of the Conference on Disarmament, and support the efforts to start substantive work, inter alia, based on the updated draft treaty on the prevention of the placement of weapons in outer space and of the threat or use of force against outer space objects submitted by China and the Russian Federation.
2. BRICS countries can cooperate in working out common approaches to ways and means of preserving outer space for peaceful purposes, which are on the agenda of the UN Committee on the Peaceful Uses of Outer Space (UNCOPUOS).

As the CD remains blocked and no substantial work is being held, there is a need to continue to push for the development of legally binding instruments to prevent weaponization of outer space. BRICS countries could start with convening an international conference to discuss the issue with other states with significant space presence.

V. Fighting Corruption as a Global Challenge to Security

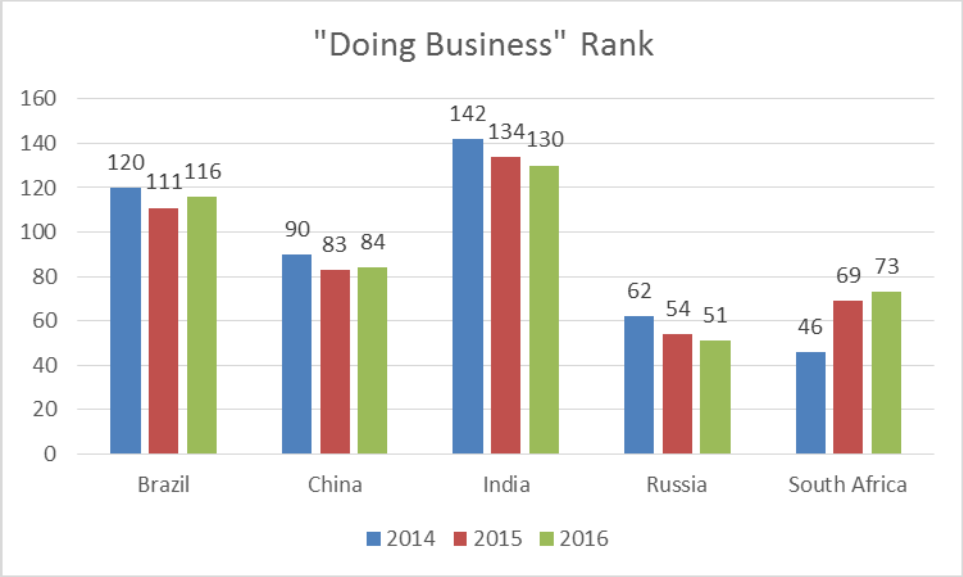
Addressing a set of hard security issues mentioned above would be already quite a heavy load for BRICS.

However, it would be fair to say that soft security challenges affect the security environment of BRICS countries more significantly than ever before. Some of our countries feel it currently with particular pain.

It is unfortunate – but it is also a fact of life – that corruption is high on this agenda in each of our nations, and it is a stigma for our societies putting a great burden on our economic and social development.

As a member of the Board on Prevention of Corruption at the Anti-Corruption Department of the Russian president's Office, I must say that the levels of corruption in my own country remain worrisome. We address this issue on the national level, at the same time examining international experiences and learning from others.

Economic Rankings of the BRICS Countries in the period of 2014-2016



Source: based on data from official website of the "Doing Business" by World Bank Group[15]

Corruption by Country[16]

[15] Economy Rankings, "Doing Business", World Bank Group, <http://www.doingbusiness.org/rankings>, last accessed September 13, 2016.

[16] Corruption by country, TRANSPERANCY INTERNATIONAL Web site, <http://www.transparency.org/country/>, last accessed September 13, 2016.

	Corruption Perceptions (2015)		Control of Corruption (2010)	Bribe Payers Index (2011)	
	Scores range from 0 (highly corrupt) to 100 (very clean).		Point estimates range from about -2.5 to 2.5. Higher values correspond to better governance outcomes.	Scores range from 0 to 10, indicating the likelihood of firms headquartered in these countries to bribe when operating abroad. The higher the score for the country, the lower the likelihood of companies from this country to engage in bribery when doing business abroad.	
	Rank	**Score**		**Rank**	**Score**
Brazil	78/168	38/100	60 %	14/28	7.7/10
China	83/168	37/100	33 %	27/28	6.5/10
India	76/168	38/100	36%	19/28	7.5/10
Russia	119/168	29/100	13 %	28/28	6.1/10
South Africa	61/168	44/100	61 %	15/28	7.6/10

When we held a conference at the Russian Diplomatic Academy on BRICS in preparation for the Ufa 2015 Summit, we decided to devote a special session to anti-corruption policies, practices, and coordination[17].

In Ufa last year, our leaders agreed that "corruption is a global challenge which undermines the legal systems of states, negatively affects their sustainable development and may facilitate other forms of crime. We are confident that international cooperation plays a pivotal role in countering and preventing corruption. We reaffirm our commitment to make every effort to that end, including mutual legal assistance, in accordance with the UN Convention against Corruption (UNCAC) and multilaterally established principles and norms"[18].

The sixth session of the Conference of State parties to the UNCAC took place in St. Petersburg on 2-6 November 2015, with active and constructive participation of all BRICS countries.

In November 2015, Russia, with the support of the BRICS countries, promoted in the UN the document on public-private partnership (PPP), aimed at combating corruption[19]. The purpose of the document is the promotion of partnership between the state and business, not only for passive protection of the business community from corrupt practices, but also to stimulate business in fighting against corruption.

As a result of the Ufa Summit, a BRICS Working Group on AntiCorruption Cooperation has been established. It is essential to support its work, with the

[17] Conference on Global Security on the BRICS Agenda for 2015: From Fortaleza to Ufa. Diplomatic Academy. Ministry of the Foreign Affairs of the Russian Federation. Moscow. 12 December 2014
[18] Seventh BRICS Summit. Ufa Declaration. July 9, 2015.
[19] BRICS offer to use the public-private partnership in fighting against corruption, Official Website of Russia's Presidency in BRICS, November 15, 2015, < http://brics2015.ru/news/20151105/656637.html>, last accessed September 15, 2016.

understanding that this issue should be of high priority; non-politicized; and not used by external forces as a pretext for intervention into our internal affairs.

Strong leadership and decisiveness in fighting corruption with no exception to the rule should be two key factors facilitating the way forward.