SECURITY INDEX

No. 2 (107), Spring 2014

Publisher: PIR Center

CSTO: COUNTERING TERRORISM CHALLENGES
FUTURE OF THE INF TREATY
RUSSIA REARMS: AN OUTLOOK TO 2020
LESSONS OF MYANMAR MANIA
FUSION OF HUMAN AND COMPUTER?
RUSSIA AND SOUTH-EAST ASIA: TOWARDS NUCLEAR PARTNERSHIP

Nikolay Bordyuzha
Evgeny Buzhinsky
Yuri Fedorov
Olga Skorokhodova
Dave Evans
Ivan Zolotukhin

2,844
March 1, 2014
2,815
April 1, 2014
2,796
May 1, 2014
2,776
June 1, 2014
2,767
July 1, 2014
2,758
August 1, 2014

Publisher
PIR Center
Andrey A. Baklitksy, Internet Program Director
Evgeny P. Buzhinsky, Lieutenant General, Senior Vice President, PIR Center
Executive Board Chairman
Alexander Y. Chepeleva, Database Coordinator
Oleg V. Demidov, International Information Security and Global Internet Governance Program Director and Editor of the Global Edition, Security Index
Julia Diamond, Intern
Dmitry G. Evtufiev, PIR Center Executive Board Member
Yuri I. Fedorov, Dr., PIR Center Executive Board Member
Galina R. Bragmova, Consultant
Natasha N. Kalinina, Dr., PIR Center Executive Board Member
Dmitry A. Kovachev, Consultant
Vadim B. Koryakin, Dr., Senior Research Fellow
Kristina O. Kuchueva, Intern
Vasily F. Lata, Lieutenant General, Consultant
Evgeny P. Maslin, Colonel General, PIR Center Executive Board Member
Vladimir A. Mau, Dr., PIR Center Executive Board Member
Vladimir A. Orlov, Dr., PIR Center Director and Executive Board Member
Evgeniya A. Pavlova, Assistant to the Director
Dmitry V. Polikarpov, Dr., Vice President
Evgeny A. Popov, IT Specialist
Galina D. Raskazkova, Accountant
Ekaterina S. Sizkova, PIR Center Projects Coordinator
Maxim V. Starshak, Assistant to the Editor-in-Chief, Security Index journal
Yekaterina A. Stepanova, Dr., PIR Center Executive Board Member
Vyacheslav I. Trubnikov, General of the Army, PIR Center Executive Board Member
Vyacheslav A. Zaytsev, Chief Accountant
Albert F. Zulkhameev, Executive Director

Website: http://si.pircenter.org/eng

Editorial policy
- No part of Security Index may be reproduced in print, electronically, or in any other form without prior written permission in writing from the PIR Center.
- The published materials, assessments, and conclusions may not necessarily coincide with the opinion of the editors and are the opinions of the authors alone.
- The editorial work on this issue was finished and approved for printing on August 29, 2014.

© PIR Center, 2014
A Russian Journal on International Security

Published since November 1994 (1994–2006 under the title Yaderny Kontrol)

Global Edition

The academic and policy quarterly journal of the PIR Center

Non multa, sed multum

SECURITY EX

No. 2 (107), Volume 20
Spring 2014

Editorial Board
Vladimir A. Orlov, Editor-in-Chief
Sergei B. Brilev
Vladimir Z. Dvorkin
Konstantin von Eggert
Dmitry G. Evstafiev
Yuri Y. Fedorov
Vasily F. Lata
Yevgeny P. Maslin
Azer A. Mursaliev
Dmitry V. Polikanov
Sergei E. Prikhodko
Sergey A. Ryabkov
Nikolai N. Spassky
Ekaterina A. Stepanova
Michael V. Yakushev

ISSN 1993-4270

Moscow • Geneva • Monterey
FROM THE EDITOR

1 Global Trends, Today's Bizarre Geopolitics, and What it Means for Russia and the World – Vladimir Orlov

A century after the First World War began, Europe and its security are now shaken by the New Cold War. It is a multistakeholder-cold-war, different from the previous one, which took place on a bipolar world, – and yet equally dangerous. Factors that brought it to life include flourishing chaos in cyberspace, development of new types of weapons, and mounting uncertainties with regard to existing global or cross-regional organizations, clubs and alliances, including the UN. Their combination leaves quite little room for optimistic expectations concerning the near future of global processes.

LETTERS TO THE EDITOR

5 Congratulations to the PIR Center on its 20th Anniversary – Sergei Ivanov, Sapar Isakov, Andrey Kolesnikov, Andrey Krutsikkh, Sergey Lavrov, Sergei Prikhodko, Sergei Shoigu, Alexander Sinaisky, Anatoly Torkunov, Vladimir Voronkov, Mikhail Ulyanov, Linten Brooks, Tariq Rauf

INTERVIEW

19 Militants and Terrorists Must Not be Allowed to Build a Social Base Inside the Csto Countries – Nikolay Bordyuzha

What are the key issues in focus of the agenda of the Collective Security Treaty Organization (CSTO)? How has the structure and the governance model of the CSTO changed over the recent years, and what new priorities have emerged for its members? These questions also touch upon the evolving approach of the Organization towards countering the challenges to regional security, fueled by the international terrorism, extremism and others threats which highlighted by the CSTO Secretary General in his interview.

23 Is the Mankind on the Way Towards Technological Singularity? – Dave Evans

The information technology revolution is going on, transforming the landscape of global development and international security in an unprecedentedly fast way. From 3D printing and augmented reality to cyborgization and predictive analytics, the digital technology generates new opportunities and new challenges for the world community. Where does this megatrend of digital progress lead the humanity? Should we get prepared for adapting familiar social,
economic and security processes to the rise of artificial intelligence and the prologue of technological singularity?

**ANALYSIS**

31 Middle East Militarization: Russia’s Role (Article II) – Natalia Kalinina

The role of Middle East in the Russian arms trade grows, with the region accounting for 20 percent of total Russian arms export and being second after the Asia Pacific. However, within this complicated region the market strategies, barriers and the demand compositions vary greatly, making successful competitive approach even more difficult. From the Gulf states with a market, quite restricted for the "newcomers", to Israel, where Russia performs in quite unusual role of arms importer, single bullet strategies are not within view. Operating with a remarkably broad selection both in terms of geography and the arms trade market niches, the author concludes the comprehensive picture of Russia's impact on the ongoing process of militarization in the Middle East region. The first part of this analysis was published in Security Index No. 4 (105) Fall 2013.

47 Myanmar Mania and the Lessons for Russia – Olga Skorokhodova

Over the recent years, Myanmar made several steps on a winding path of economic and political transformations. The government made a bid on opening of the national economy in order to attract foreign investors, and this strategy resulted in impressive investment boom. However, the experience of several years of Myanmar mania also reveals pitfalls and peculiarities of massive investments in this new national market. The current experience of major powers' cooperation with Myanmar offers valuable lessons for Russia. Moscow and Naypyidaw share a significant historical background of economic and trade cooperation, and have perspective tracks and formats of its further development – but only if the mutual risks are well understood and mitigated.

61 Russia and the Southeast Asia: Towards Nuclear Partnership – Ivan Zolotukhin

Amid the ongoing confrontation with the West, Russia’s foreign-policy course is pivoting towards the East, with the growing market of the South-East Asia promises opportunities for partnership in a number or areas, including peaceful nuclear energy industry. At the same time, Russia remains a guest in the region and it still must work out a formula of its involvement and participation in Southeast Asia. A successful strategy for cooperation with the regional countries should take into account major risks and challenge in the region such as the Fukushima syndrome, the lack of human resources and increasing competition both with alternative sources of energy and foreign market actors in the nuclear energy segment.

**DOSSIER**

71 Outcomes of the Russian-US High-Level Working Group on the Iranian Nuclear Issue – Andrey Baklitsky

The article provides a set of proceedings of the meeting of the Russian-US working group on Iranian nuclear issue, which was established in November of 2013 by PIR Center and the Near East South Asia Center for Strategic Studies (NESA). The meeting of the group that took place in Gstaad, Switzerland and was later supplemented by the coordinators’ work in the first half of 2014, pursued the aim of supporting the positive dynamics of the process of negotiations between Iran and P5+1 and contributing to reaching of the Comprehensive agreement on the Iranian nuclear program. The multifold set of expert views and recommendations provides
an elaborated algorithm for all sides on the path towards the Comprehensive Agreement and the final resolution of the deadlock over the Iranian nuclear issue.

**ROUNDTABLE**

75 **Common Agenda for Russia and ASEAN in Cyberspace: Countering Global Threats, Strengthening Cybersecurity, and Fostering Cooperation**  
- Boris Vasiliev, Alexander Kalinin, Alexey Lukatsky, Mikhail Medrish, Vladimir Orlov, Viktor Tarusin, Mikhail Yakushev, Andrey Yarnykh

Over a year after the 2013 APEC summit in Vladivostok, Southeast Asia retains and enhances its appeal to Russia as a promising platform for growing trade and economic ties. At the same time, against the backdrop of growing contradictions with the West, the regional actors in Southeast Asia, including ASEAN, are becoming increasingly important potential partners for Russia both in terms of economic and security cooperation. One major field of such cooperation is cybersecurity, observed under a two-fold perspective of trade cooperation and promotion of Russian solutions to the boosting, though highly competitive regional market, and strategic dialogue with the ASEAN states on ensuring the security of cyberspace on global and regional level. To succeed, the Russian side needs not only highest concentration of political will and diplomatic efforts, but effective engagement of private businesses and experts into its move to the ASEAN market.

**COMMENTARY**

89 **Does The INF Treaty Have a Future?**  
- Evgeny Buzhinsky

The expert community is increasingly raising the question of whether Russia should withdraw from the 1987 Intermediate-Range and Shorter-Range Nuclear Forces Treaty (INF) today. Potential Russia’s pullout from the Treaty has been discussed since 2003. The issue remains controversial as the treaty is claimed to be detrimental to Russian national security. At the same time, the idea of initiating the collapse of yet another disarmament treaty raises serious concerns over its probable impact on strategic stability. Besides, a thorough analysis shows that unlike the ABM Treaty, the INF Treaty does not hamper Washington’s defense plans, and this fact leaves certain window of opportunities for the Treaty’s future.

95 **Russian Armament Program 2020: Current State and Outlook**  
- Yuri Fedorov

The implementation of the State Armament Program to 2020 in Russia results in a massive renovation of weapons and military equipment in a scale, which is unmatched in the modern Russian history. The ambitious program reflects the undisputable priority of technologically upgraded and strengthened Armed Forces. However, the question remains open on how realistic the SAP-2020 targets and plans are – and it becomes even more topical as the international situation undergoes extensive deterioration. Can the Russian defense industry deliver such a massive increase in defense R&D and manufacturing under the press of sanctions? These questions also become vital for further progress of the SAP-2000 and successful launch of the new armaments program for the 2016–2025 period.

103 **The CTBT and Strategic Relations between Russia, China, and the United States**  
- Nikita Perfiliev

Even though the Comprehensive Nuclear-Test-Ban Treaty has not yet entered into force, it already influences nuclear disarmament and nonproliferation in several practical ways. Those include increasing barriers for the would-be...
nuclear proliferators, placing constraints on the modernization of nuclear arsenals of the established nuclear weapons' possessors and stimulating progress towards a world without nuclear weapons. At the same time, the perspectives the Treaty's entry into force largely revolve around its ratification by China and the USA, with Russia's approach to the already ratified Treaty also being taken into account. But regardless of the ratification bargaining and debates, development of the CTBT mechanism depends on achieving such practical goals as ensuring transparency of nuclear test sites and facilities.

Developing National Regulations to Support Nuclear Security: Lessons Learned from the U.S. Support to Russia, Ukraine, and Belarus – Dmitry Kovchegin

Development of national regulations supporting nuclear materials control and accounting and physical protection is a major part of ensuring states compliance with requirements of the United Nations Security Council Resolution 1540, with the IAEA playing a central role in this process. In case Russia, as well as Belarus and Ukraine after collapse of the Soviet Union, the process of elaboration of such regulations took place with a major contribution from the USA. The cases of the three countries which take into account the peculiarities of the regulatory environment and the process of developing capabilities necessary to establish the requirements, provides valuable experience which should be reassessed now, when the U.S. support in this field is going to become a turned page of history.

REVIEW OF RECENT WORLD EVENTS

International Security Index in January–June 2014: Cold Reality 2.0 – Galiya Ibragimova

The first half of 2014 was marked with dramatic changes in the landscape of the international relations and global security. The new Cold reality rapidly has emerged from the global and regional trouble spots, including the chaos in the Middle East, deteriorating conflict in the east of Ukraine, and maintaining geopolitical tension in the East Asia. The turbulent international environment affects Russia, but still goes far beyond any national borders. Galiya Ibragimova highlights the worrying banking turns of the International Security Index at this geopolitical rollercoaster.

ICT in the BRICS Agenda before the 2015 Summit: Installing the Missing Pillar? – Oleg Demidov

The BRICS states that today together account for over 900 mln internet users, remain underrepresented in the global internet governance discussions. To erect the ICTs as another pillar in its agenda the 'new giants' should get more engaged in the policy-making process and demonstrate well-orchestrated leadership on such issues as the IANA functions transition, reform of the multistakeholder internet governance model, etc. More opportunities are hidden on the level of joint infrastructure projects, hardware and software solutions. However, to succeed the BRICS needs Russia's input based on its well-elaborated approach to the information security and internet governance issues.

PAGES OF HISTORY

The Role of Security Assurances to Ukraine and the 1994 Budapest Memorandum: From the 1990s to the Crimea Crisis – Vladimir Orlov

Till 2014 the issue of nuclear weapons on Ukraine's territory, and of security assurances to be given to Ukraine in return for becoming a non-nuclear weapon
state, seemed to be resolved once and for all in the Trilateral Statement by the Russian, U.S. and Ukrainian presidents, and then in the Budapest Memorandum on Security Assurances, both signed in 1994. However, the Crimean crisis made experts and decision makers raise the question whether the Budapest Protocol is still in force and what are the implications of potential answer for Ukraine; Crimea; and each of the three states that gave Ukraine the security assurances. The author of the article provided a retrospective analysis of the issue observing the Crimean crisis from half a year's distance.

141 ABOUT THE AUTHORS

FINAL QUOTES

On Awe-Inspiring Progress
GLOBAL TRENDS, TODAY'S BIZARRE GEOPOLITICS, AND WHAT IT MEANS FOR RUSSIA AND THE WORLD

NATO left Afghanistan.

Putin took nash Cream.

Cristina Kischner took the Union Jack

(not yet)

Final Cut UPD

A century after the First World War began, Europe—in a broader meaning of a Euro-Atlantic space from Vancouver to Vladivostok—and its security are now shaken by the New Cold War. It is a bizarre cold war as the bipolar world order—the type of world order accustomed to cold war—was gone 25 years ago. It is a new era of multistakeholder-cold-war.

The fact it is bizarre does not make it less dangerous than the “traditional” cold war of the past. Finally, the same actors as 25 years ago still have nukes. Unlike 25 years ago, though, they have the most sophisticated types of lethal and non-lethal weapons. This cold war is not just a post-Ukraine-crisis hangover episode. We should get prepared for a long, shaky, and chilly period of political instability and conflict.

This multistakeholder-cold-war has several major characteristics; one of them is chaos, fear, and an arms race in cyberspace. The internet is still quasi-free, but de facto controlled by its original designer—the United States and its military—with little prospect of a new global internet governance. The Snowden revelations have only been the tip of the iceberg. More than 120 states are working on cyber weapons or have active offensive/defensive cyber programs.

Moreover, even the multilateral efforts to promote cooperation and confidence building in a cybersecurity area in such a dynamic and viable format as the ASEAN Regional Forum are still in the initial stage of development and can be crippled by exacerbating the turbulence in international relations. For more details please read the roundtable on Russia—ASEAN cooperation in cybersecurity area.

Apart from cybersecurity issues, the ASEAN region appears to be a safe haven in today’s turbulent world for some priority dimensions of Russia’s foreign policy—as it makes the case with Russia—ASEAN cooperation in the nuclear sphere, which is analyzed by Ivan Zolotukhin. But neither this positive engagement potential, nor the sweet temptation to fall into Myanmar mania (examined by Olga Škorokhodova) is able to balance the global tsunami of instability which Russia is facing together with the rest of the global community.

In addition, everything is ready for an arms race in outer space. International, particularly Russia–US space cooperation, active for 20+ years, is now gone. The United States, China, Russia, India, and possibly other major players are ready to jump into outer space with ambitious plans that would anyway, even if they are not overtly military, affect global
security—adding more global insecurity and vulnerability not only for those who do not play in star wars and other space games, but for all.

Finally, the deterioration of the international situation includes mounting uncertainties with regard to existing global or cross-regional organizations, alliances, clubs, and coalitions, and their reshaping.

☐ The United Nations is completely confused regarding international law norms and sinking even further into a global-bureaucracy swamp.

☐ NATO has practically failed in Afghanistan and is largely driven by Poland and the Baltics in their search for a “new old” enemy in the counterproductive context of the Ukrainian crisis.

☐ The Collective Security Treaty Organization (CSTO) largely remains a sleeping structure in the global security architecture. Very few people even know what it stands for, while the organization is having a ridiculously low influence in the regions where it may be crucial such as Central Europe, the Caucasus, and Central Asia. However, the Secretary General of the CSTO Nikolai Bordyuzha provides some valid arguments against utter pessimism concerning the CSTO and its prospects in his interview for the Security Index journal.

☐ The G8 is now gone after the outbreak of the Crimea crisis—and even well before the deterioration of the conflict in the east of Ukraine.

☐ BRICS is one of the few international coalitions that is still trying to appear dynamic, even looking for expansion into Argentina and Turkey...but in reality it is facing growing contradictions among its members. BRICS unity will be tested very soon at the summit in Brazil’s Fortaleza. The contrast between BRICS ambitions and the divergence of the approaches practiced by its members is perfectly revealed in the field of global internet governance and cyber governance. The strategies of the non-Western giants’ forum in this field and their prospects in the light of the BRICS summit of 2015 in Ufa are highlighted by Oleg Demidov.

Ukraine was not the major reason but just a “final drop” in US-Russian relations. However, that was a significant “drop”, too painful and too poisonous for Russia to digest. The coup d’État in Kiev in February 2014 orchestrated by Washington was a classical one, tested many times before in places like Latin America, Africa, and the Middle East—but the closest to the Russian borders and most vital ever to Russia’s interests. Moscow acted swiftly and professionally on Crimea though the same idea of challenging or changing Helsinki-born principles and the status quo was something alien to Moscow even a few months ago. Now, there is a civil war in Ukraine, with a risk of having a low-to-high-intensity conflict there for many years.

The Ukraine crisis has had a dramatic effect on Russian domestic policy as well, giving a unique chance to those who have always been on the margins of the Kremlin decision-making: ultra-cons, Orthodox fundamentalists whose ideology is anti-Western in itself, and will continue to be so, whatever happens next in or around Ukraine. Putin’s long-term course towards the saving of his own and his country’s energy, expended on useless quarrels, and investing in development instead—this course has been torpedoed and significantly damaged. In that sense, the Obama administration has achieved its very shortsighted, but clear and familiar goal: they weakened Russia again, by successfully provoking it to demonstrate its power.

On the other hand, this is Russia’s hard, raw power—and President Putin’s unquestionable strength itself—that now attracts important players from the Middle East and East Asia, as well as other regions, who are more eager to do business with Russia today than ever before—Japan may be the best example but definitely not the only one.

In his July 2014 speech addressed to Russian ambassadors, President Putin deliberately chose a conciliatory, moderate tone. Without allowing any concessions vis-a-vis Ukraine and the West, and rightly so, Putin preferred to concentrate on constructing a Eurasian Union as a common economic (and, perhaps, in a future—a geopolitical) space—his favorite project considerably shaken by the Ukraine crisis but still alive and with a certain potential.

As some European observers have already correctly noted, President Putin’s pragmatism should not allow him to go too far towards the new Cold War and to appease those in his

NOTES

1. With thanks to K. Galley for help with these notes.
team who, with limited vision and limited creativity, still push their own hawkish foreign policy agenda. At the same time, it is true that they are the true winners of the Crimea operation, and their growing appetite for power within the decision-making process cannot simply be ignored or downplayed. Thus, Putin will have a search for a fine line between damage to Russia’s development and playing down his increasing anti-Western feelings-turned-philosophy.

So what expectations should we have in the light of the Cold Reality 2.0 (as it was termed by Galiya Ibragimova in the international Security Index in the first half of 2014)?

First, the existing security treaties will be questioned, some of them will die soon, some will die hard, and some of the most essential, like the NPT, may even survive but without any chance of strengthening. Evgeny Buzhinsky provides a bright illustration of this trend in his examination of the questionable future of the Intermediate-Range Nuclear Forces Treaty of 1987.

Second, new multilateral treaties dealing with new global threats and phenomena such as the cyber- and outer space arms race will be very unlikely in the current shaky and tense environment.

Third, formal international organizations such as the UN and its institutions as well as the informal coalitions and “clubs” of nations—be it the G7 or BRICS—will not be capable of dealing with or adequately addressing this global security agenda.

Therefore and finally, the impression of the last decades that hard power is reducing its role compared with soft power proved not only wishful thinking, not simply wrong, but dangerously misleading. The global processes have gone berserk, and we are doomed to increasing global instability.

As sad as it sounds, one can hardly ever find a panacea to prevent this destabilization—and this is truly the bad luck of today’s world.

Vladimir Orlov

NOTE

1 With acknowledgement to Pink Floyd.
Letters to the Editor

CONGRATULATIONS TO THE PIR CENTER ON ITS 20TH ANNIVERSARY

TO THE PIR CENTER PRESIDENT
DR VLADIMIR ORLOV

Dear Dr Orlov,

I would like to extend my sincere congratulations on the occasion of the PIR Center’s 20th anniversary.

Over the years, the PIR Center has firmly established itself among the leading Russian non-governmental organizations, specializing in issues of international security, nuclear non-proliferation, and arms control. The high level of professionalism of the PIR Center staff and the effectiveness of organization of their work has earned the Center a high level of prestige in political, academic, and social circles both in Russia and abroad.

Your research serves as a significant support to the work of the Presidential Executive Office, as well as for many ministries and departments of the Russian Federation. The intensive analysis and publishing activities of the Center are an excellent example of constructive cooperation between the expert community and the government. I am confident that this collaboration will continue to develop successfully.

Respectfully,

Sergei Ivanov
Chief of Staff
Presidential Executive Office of the Russian Federation
23/16 Ilyinka str.
Moscow, 103132, Russia
TO THE PIR CENTER PRESIDENT
DR VLADIMIR ORLOV

Dear Dr Orlov,

Please accept my sincere congratulations on the 20th anniversary of the PIR Center.

In that relatively short time, the organization that you lead has produced a huge amount of studies on a wide range of international security issues, including nuclear nonproliferation and arms control. Today the PIR Center is duly recognized as an influential research and training think tank that conducts serious research, implements a number of challenging projects, develops recommendations on strategically important areas of international security, and trains a new generation of experts in international affairs.

We value the constructive cooperation that we have established with the PIR Center in recent years. The International Summer Schools on Global Security, annually conducted by your organization, spark high interest among our staff, while the Security Index journal is an important source of well-balanced information. We would like to express our sincere gratitude to you and look forward to further cooperation in all the relevant areas.

We wish the PIR Center team success, wellbeing, prosperity, and all the best.

Sincerely yours,

Sapar Isakov
Deputy Chief of Staff
Kyrgyzstan Presidential Staff
205 Chiu avenue
Bishkek, 720003, Kyrgyzstan

TO THE PIR CENTER DIRECTOR

Dear Mr. Anan'ev,

I am writing to congratulate you on the 20th anniversary of the PIR Center.

The PIR Center is an distinguished institution of international affairs, and your Center has made an important contribution to the development of the field. The Center's work has been recognized both at home and abroad, and its impact is evident in the many initiatives and projects it has undertaken over the past two decades.

I would like to congratulate you and the PIR Center on this milestone and express my hope that the Center will continue to thrive and make important contributions to the field of international affairs.

Sincerely,

Mikhail Bogdanov
Deputy Director
Central Asia Institute of Economics and Finance

TO THE PIR CENTER PRESIDENT

Dear Dr Orlov,

I am writing to congratulate the PIR Center on its 20th anniversary.

The PIR Center has been a leader in the field of international security and has made important contributions to the development of the field. I would like to express my hope that the Center will continue to thrive and make important contributions to the field in the years to come.

Sincerely,

[Signature]
TO THE PIR CENTER PRESIDENT
DR VLADIMIR ORLOV

Dear Dr Orlov,

I am delighted to congratulate the PIR Center team on the landmark event of its 20th anniversary.

There are not many Russian NGOs that have managed to live through the challenging times of change of the public discourse in Russia and to remain a key participant in the broad international discussion on foreign policy and global security issues. In that sense, the PIR Center’s motto—"Non Multa, Sed Multum"—is particularly significant, as it highlights the noble mission that its small but close-knit and dedicated team successfully carries out practically in 24/7 format.

Collaboration with the PIR Center’s team has opened up for us, as the representatives of the Russian Internet sector, new opportunities for promoting a discussion of a whole range of issues related to global Internet governance and cybersecurity. We are cordially grateful to your colleagues for giving us an opportunity to engage in an open discussion with other stakeholders' representatives in the informal atmosphere of your Midweek Brainstorming sessions, and we hope to keep up this excellent tradition.

For you, just as for the Runet, 20 years is not a time for looking back but a time for setting new ambitious goals. We wish the PIR Center to remain at the center of events and to enjoy the respect of its peers in all research fields and on all continents where members of the diverse, multilingual, and academically ambitious international expert community live and work.

Sincerely,

Andrey Kolesnikov
Director
Coordination Center for Top Level Domains. RU./.РФ
8 Zoologicheskaya str.
Moscow, 123242, Russia

LETTERS TO THE EDITOR
TO THE PIR CENTER PRESIDENT
DR VLADIMIR ORLOV

Dear Dr Orlov,

I would like to congratulate the PIR Center on its 20th anniversary.

For a non-governmental organization engaged in international security research, 20 years is not just an impressive figure but also evidence of the high relevance of its work.

The PIR Center can take rightful pride in being one of the first non-governmental think tanks to engage in thorough research on the issues of international information security and global Internet governance.

The expert community always meets the PIR Center’s publications with praise, as they highlight the growing significance of issues concerning the development of information and communication technologies in the context of international security.

I would like to encourage the PIR Center to continue building on the results it has already achieved and to pursue further research in this field.

I also wish you and PIR Center to keep up the achieved quality of studies, and uphold the traditions of foreign policy research that not only meet high academic standards but also contribute to strengthening Russia’s national security.

Sincerely yours,

Andrey Krutskikh
Special Representative of the President of the Russian Federation for international cooperation in information security, Ambassador-at-large
Ministry of Foreign Affairs of the Russian Federation
32/34 Smolenskaya-Sennaya sq.
Moscow, 119200, Russia
TO THE PIR CENTER PRESIDENT
DR VLADIMIR ORLOV

Dear Dr Orlov,

I am pleased to congratulate the PIR Center on the occasion of its 20th anniversary. For the last 20 years, your organization has played a vital role in the field of security research, stimulating debate on the most pressing issues of international relations and striving to provide analytical support to Russia’s foreign policy.

Understanding international processes is impossible without an academic approach. However, the ever-changing global situation requires a rapid, accurate response. The PIR Center has been able to successfully strike a balance between theory and practice, which provides excellent analysis.

I deeply appreciate the work of the PIR Center and wish your organization continued success in your endeavors.

Respectfully,

Sergei Prikhodko
Deputy Prime Minister of the Russian Federation
Chief of Staff
Government of the Russian Federation
2 Krasnopresnenskaya Naberezhnaya
Moscow, 103274, Russia

TO THE PIR CENTER PRESIDENT
DR VLADIMIR ORLOV

Dear Dr Orlov,

I am pleased to congratulate the PIR Center on the occasion of its 20th anniversary. For the last 20 years, your organization has played a vital role in the field of security research, stimulating debate on the most pressing issues of international relations and striving to provide analytical support to Russia’s foreign policy.

Understanding international processes is impossible without an academic approach. However, the ever-changing global situation requires a rapid, accurate response. The PIR Center has been able to successfully strike a balance between theory and practice, which provides excellent analysis.

I deeply appreciate the work of the PIR Center and wish your organization continued success in your endeavors.

Respectfully,

Sergei Prikhodko
Deputy Prime Minister of the Russian Federation
Chief of Staff
Government of the Russian Federation
2 Krasnopresnenskaya Naberezhnaya
Moscow, 103274, Russia

TO THE PIR CENTER PRESIDENT
DR VLADIMIR ORLOV

Dear Dr Orlov,

I am pleased to congratulate the PIR Center on the occasion of its 20th anniversary. For the last 20 years, your organization has played a vital role in the field of security research, stimulating debate on the most pressing issues of international relations and striving to provide analytical support to Russia’s foreign policy.

Understanding international processes is impossible without an academic approach. However, the ever-changing global situation requires a rapid, accurate response. The PIR Center has been able to successfully strike a balance between theory and practice, which provides excellent analysis.

I deeply appreciate the work of the PIR Center and wish your organization continued success in your endeavors.

Respectfully,

Sergei Prikhodko
Deputy Prime Minister of the Russian Federation
Chief of Staff
Government of the Russian Federation
2 Krasnopresnenskaya Naberezhnaya
Moscow, 103274, Russia

TO THE PIR CENTER PRESIDENT
DR VLADIMIR ORLOV

Dear Dr Orlov,

I am pleased to congratulate the PIR Center on the occasion of its 20th anniversary. For the last 20 years, your organization has played a vital role in the field of security research, stimulating debate on the most pressing issues of international relations and striving to provide analytical support to Russia’s foreign policy.

Understanding international processes is impossible without an academic approach. However, the ever-changing global situation requires a rapid, accurate response. The PIR Center has been able to successfully strike a balance between theory and practice, which provides excellent analysis.

I deeply appreciate the work of the PIR Center and wish your organization continued success in your endeavors.

Respectfully,

Sergei Prikhodko
Deputy Prime Minister of the Russian Federation
Chief of Staff
Government of the Russian Federation
2 Krasnopresnenskaya Naberezhnaya
Moscow, 103274, Russia
TO THE PIR CENTER PRESIDENT
DR VLADIMIR ORLOV

Dear Dr Orlov,

On behalf of the Secretariat of the Defense Ministers Council of the Commonwealth of Independent States, allow me to convey our heartfelt congratulations to you and your staff on the 20th anniversary of the PIR Center!

Over these years, the PIR Center has become one of Russia’s leading organizations engaged in multifaceted work in the field of international security.

Thanks to your efforts, a unique research and education framework has been created and is successfully developing, where young national and global security experts expand their professional horizons and acquire new knowledge.

The PIR Center’s research and education projects are renowned for the variety of topics they cover; for their creative approach and use of cutting-edge technologies; as well as for their reliance on discussion and dialogue in debating the most topical issues of the modern day. Many years of close and fruitful cooperation with leading Russian and foreign experts have enabled the PIR Center to build a highly professional team of lecturers, who have profound knowledge and extensive experience of national and regional security issues.

Your efforts to carry our education programs among young politicians, diplomats, officers, and journalists meet with great interest in the CIS member states.

I hope that mutually beneficial cooperation between the PIR Center and CIS member states’ defense ministries will contribute to preserving common values in ensuring regional security, promoting good-neighborly relations, and mutual understanding within the CIS.

I wish the PIR Center team wellbeing and prosperity and further success in their work for the benefit of the Russian Federation, the Commonwealth of Independent States, and the whole international community.

Sincerely yours,

Alexander Sinaisky
Head of the Secretariat
Defense Ministers Council of the Commonwealth of Independent States
41 Leningradsky avenue
Moscow, 119160, Russia
TO THE PIR CENTER PRESIDENT
DR VLADIMIR ORLOV

Dear Dr Orlov,

Congratulations to the employees of the Russian Center for Policy Studies on the organization’s 20th anniversary. For twenty years, the Ministry of Defense of the Russian Federation has received from the PIR Center strong analytical support on the issues of nuclear nonproliferation and arms control.

In today’s world, the military potential of a country is measured not only by the number of tanks and planes it has, but also by its intellectual resources. I am pleased to note that Russian research institutes, such as your Center, help us to maintain and create opportunities in this area. Creation of a training center on international security with a decision of the Council of Defense Ministers of the Commonwealth of Independent States has been just one shining example of the PIR Center’s work in strengthening international military cooperation.

I wish you continued success in your work.

Respectfully,

Sergei Shoigu
Minister, General of the Army
Ministry of Defense of the Russian Federation
19 Znamenka str.
Moscow, 119160, Russia
TO THE PIR CENTER PRESIDENT
DR VLADIMIR ORLOV

Dear Dr Orlov,

On behalf of MGIMO University, I sincerely congratulate you and all of your colleagues at the PIR Center on your 20th anniversary!

The PIR Center has managed to become the leading expert-analytical organization in Russia on issues of international security and the nonproliferation of nuclear weapons. The highly professional work of PIR Center analysts makes a significant contribution to the development of applied scientific research on strategically important international problems.

Furthermore, I would like to express my gratitude for your efforts to integrate ongoing PIR Center research into the educational process at MGIMO University. The joint module on nuclear nonproliferation that was organized in 2013 sparked lively and interested feedback from students and demonstrated great potential for future cooperation. We hope that the grounds we created will serve as a foundation for the opening of full-fledged education and training programs.

I wish you and all of your colleagues at PIR Center wellbeing, further creative and scientific success, and fruitful work.

Sincerely,

Anatoly Torkunov
Rector
Moscow State Institute of International Relations (University) of the Ministry of Foreign Affairs of the Russian Federation
76 Vernadsky avenue
Moscow, 119454, Russia

LETTERS TO THE EDITOR

SECURITY INDEX No. 2 (107) Volume 20
TO THE PIR CENTER PRESIDENT,
EDITOR IN CHIEF OF THE SECURITY INDEX JOURNAL
DR VLADIMIR ORLOV

Dear Volodya,

I would like to warmly congratulate you and the PIR Center’s team on your anniversary! Twenty years is not just an impressive figure and a good reason to take stock of the journey so far. It is, first and foremost, a significant landmark, clearly showing that the PIR Center has truly come into its own, becoming a valued and highly sought actor in its field. It is also an opportunity to look into the future, open up new horizons, set new ambitious goals, and formulate long-term tasks.

I could say a lot about the virtues of the PIR Center not only as an influential analytical platform but de facto as a Russian brand, an internationally recognizable mark of quality in nuclear nonproliferation, disarmament, and international security studies. What has always set the PIR Center apart and what we particularly appreciate is its readiness to cooperate with the Russian governmental agencies, in particular the Ministry of Foreign Affairs. Of course, our views and approaches to various issues do not always coincide. However, the PIR Center’s viewpoint is always of interest and value. Over the past 20 years the PIR Center has built a unique team and formed a distinctive view on the most complex and sensitive issues of the so-called hard power, which allows it to come up with competent proposals for overcoming today’s global challenges. This is what our productive cooperation is based on.

A particularly important role belongs to the PIR Center’s training projects, especially its annual International Summer Schools on Global Security. They help to train a new generation of international security experts, who, having gained useful practical experience inside the PIR Center, become proficient in such complicated matters as nuclear nonproliferation and disarmament. Even more importantly, these projects bring together experts from the Commonwealth of Independent States and East European countries and contribute to promoting the Russian language and strengthening its positions in this part of the world. This is our common task.

We are entering a challenging period in international relations. Attempts are being made to undermine the established norms of interaction between states and to impose an egoistic interpretation of international law in a bid to restore a monocentric world. This policy is breeding chaos. That is why together we shall have to address the difficult tasks of preserving stability in international relations and reinforcing the universal understanding that the only way to resolve modern problems lies through international law. We hope that we shall be able to continue to rely on professional support from the PIR Center.

I wish you and your team further success and new achievements.

Sincerely yours,

Vladimir Voronkov
Permanent Representative, Minister Extraordinary and Plenipotentiary
Permanent Mission of the Russian Federation to the International Organizations in Vienna
182 Erzherzog-Karl-Str.
1220, Vienna, Austria

CONGRATULATIONS TO THE PIR CENTER ON ITS 20TH ANNIVERSARY
TO THE PIR CENTER PRESIDENT
DR VLADIMIR ORLOV

Dear Dr Orlov,

We congratulate you and your staff on the 20th anniversary of the PIR Center!
Throughout all these years, the PIR Center has repeatedly demonstrated that it is duly recognized as one of Russia's most influential NGOs, with great political potential and solid expertise.

We appreciate our close and fruitful cooperation with your organization on the issues of arms control, nonproliferation, and disarmament, and look forward to its further development.

We wish you and your team continued success and enthusiasm for defending Russia’s national interests in the international arena!

Sincerely yours,

Mikhail Ulyanov
Department Director
Department for Non-Proliferation and Arms Control
Ministry of Foreign Affairs of the Russian Federation
32/34 Smolenskaya-Sennaya Sq.
Moscow, 119200, Russia
TO THE PIR CENTER PRESIDENT
DR VLADIMIR ORLOV

Dear Volodya,

Congratulations on the 20th anniversary of the PIR Center.
You have given it an international reputation and made it one of the most respected organizations in Russia.
All the best.

Ambassador Linton F. Brooks
9920 Chase Hill Court
Vienna, VA 22182, Austria
TO THE PIR CENTER PRESIDENT
DR VLADIMIR ORLOV

Dear Volodya,

I am exceedingly pleased to congratulate you and your colleagues on the 20th anniversary of the PIR Center's founding on April 30, 1994.

Over its two decades, the PIR Center has come to be widely recognized as the leading independent non-governmental organization and think tank working on global and regional security issues in the Russian Federation. It is not surprising that the Presidency, the foreign and defense ministries, the State Duma, civil society and the media, in the Russian Federation, all recognize the contribution of you and your esteemed colleagues at the PIR Center to strategic policy discourse within and outside the Russian Federation.

The PIR Center's prestige and excellence is not confined to the Russian Federation, indeed it has achieved global reach through its valuable work on promoting Russian–U.S. strategic dialogue, security in the Middle East, South Asia, East Asia, and in the European space, among other areas and activities.

The PIR Center has highly regarded educational, public awareness, and publishing activities. The PIR Center's periodical Security Index journal, formerly Yaderny Kontrol (Nuclear Control) has published more than 100 issues, carrying articles and opinions by senior Russian official and academicians, as well as by foreign scholars and practitioners. I am always intrigued by the logo of the journal, which is a rhinoceros—so on some pages the rhinoceros is emerging from a file folder.

There are legends concerning a rhinoceros stamping out fire in Malaysia, India, and Burma. Myths have it that the rhinoceros would come when a fire is lit in the forest and stamp it out. There are no recent confirmations of this phenomenon. However, this legend has been reinforced by the film "The Gods Must Be Crazy," where an African rhinoceros is shown to be putting out two campfires. What I take from this is that the rhinoceros in the Security Index journal is symbolically putting out the WMD fires.

Congratulations to PIR Center on its 20th anniversary! I wish you and your organization continuing success and fame.

Tariq Rauf
Director
Arms Control and Non-Proliferation Programme
Stockholm International Peace Research Institute
9 Signalstgatan
Solna, 169 72, Sweden
Against the dominating background of a deteriorating security situation in Eastern Europe, security on the southern borders of the former Soviet Union still not only remains a topical issue but risks becoming even more so following NATO’s withdrawal from Afghanistan which has started in 2014. At the same time, it is affected by the overall international security context and the expanding destabilization in the Middle East fueled by the ongoing conflict in Syria and the military successes of the Islamic State.

What tasks does the Collective Security Treaty Organization (CSTO) focus its work on to ensure the security of its member states in these uneasy circumstances? Which areas are at the top of the Organization’s development agenda now? What has changed in the CSTO management structure recently? Security Index took the chance to put these and other related questions to the CSTO Secretary General Nikolai Bordyuzha.

SECURITY INDEX: These days, the attention of the international community with regard to the Middle East region is largely focused on the situation in Iraq. However, the ongoing conflict in Syria also remains one of the key drivers for regional destabilization. How probable is a repetition of the Syrian scenario in CSTO member states?

BORDYUZHA: I regard the events in Syria as a regime-change technology, a rough version of the so-called color revolutions. Such processes tend to begin with a massive influx of propaganda among young people, followed by the establishment of communication cells, strongholds, etc., and then the Terrorist International gets down to active operations. From all parts of the world, there arrive people willing to fight, people with certain political beliefs. They are usually supplied with arms, put together in detachments or organizations, and after their arrival a war with the lawfully elected authorities often breaks out.

There are cells of Hizb ut-Tahrir al-Islami and other radical religious groups actively operating in the CSTO member states, creating a social base there to use later to achieve their political goals. Furthermore, there are reports that citizens of the CSTO states undergo intensive training in camps on the territory of Afghanistan and Pakistan. If you put all these reports together, it follows that at some point trained militants could be sent to our countries to fight against the incumbent authorities.

SECURITY INDEX: Which CSTO member states appear to be most vulnerable in this respect?

BORDYUZHA: All CSTO member states, perhaps with the exception of Belarus and Armenia, could be affected. Several months ago, a terrorist cell was uncovered outside Moscow, whose members had been trained in the Afghan camps. I think that was the first evidence of
trained people being dispatched here to destabilize the situation, and there may be more evidence of that still to come. We take these precedents into account when discussing topical threats, including the possibility of armed groups that have political goals breaking through the Tajik–Afghan border. Incidentally, international terrorist groups already took part in the events in southern Kyrgyzstan in 2010, sending their emissaries there.

SECURITY INDEX: To what extent do the ruling elites of CSTO member states, apart from Russia, share the goals, tasks, or even values of the organization? Is not their membership of the CSTO a way of securing some preferential terms, primarily from Russia, rather than a way of achieving joint strategic objectives?

BORDYUZHA: I categorically reject this interpretation. The CSTO is a voluntary organization, and all its member states joined it with their eyes open. Of course, Russia is the main donor within the CSTO, but it is not the only donor. It is just that Russia, in terms of its might and in terms of its potential, is significantly bigger than the other states and has more capabilities, including when it comes to security, so it provides assistance to its partners.

At the same time, the main principle of the CSTO is the principle of consensus. We do not have a single project that is opposed by at least one state for rational or value reasons. I could give you examples: Kazakhstan purchases all weapons, special equipment and gear with its own funds; Armenia, while receiving aid from us, purchases a considerable part of its weapons with its own funds; Belarus either produces or purchases with its own money a considerable part of its weapons. There is no Russian sponsorship there.

Indeed, Tajikistan or Kyrgyzstan do not produce weapons and, given their economic situation, seek assistance, but otherwise they would not be able to fulfill our common tasks. We created the CSTO, among other things, to have preferential terms for purchasing arms inside it, which is set out in the signed agreements. But, allow me to reiterate, no one is viewing Russia as a cash cow within the Organization.

SECURITY INDEX: What situation will the withdrawal of U.S. troops from Afghanistan create on the southern borders of the CIS? Will not Russia have to assume the role of a deterrent factor of sorts?

BORDYUZHA: First, the United States and its NATO allies are transforming their presence in Afghanistan rather than withdrawing from there altogether.

Second, we are now dealing very seriously with the challenge of maintaining stability and security of the CSTO’s southern borders after the withdrawal of the U.S. armed forces from the Afghanistan. This process, which also used to be known as the so-called Problem-2014, is now entering its active phase although we know that American bases will remain there, as will quite considerable forces. Overall, we believe that the situation will be changing for the worse and the level of instability will rise. The factors that present a certain danger for us today—militant training camps, terrorist organizations, militant groups, and laboratories producing large quantities of drugs—will remain after the withdrawal of NATO’s main contingent is completed. That is why now we need to become stronger.

Although we do not expect large-scale invasions, Russia, together with its CSTO allies, will have to take additional measures to ensure stability in these countries. For instance, at a session of the Collective Security Council in Sochi in the fall of 2013, the leaders of the CSTO member states agreed to provide Tajikistan with urgent military-technical assistance to better protect the border with Afghanistan. This decision is now being implemented together with a number of other preventive steps.

SECURITY INDEX: Are these measures largely political in nature, or are there preparations under way for military operations too? One gets the impression that the CSTO does nothing but preparations, given its non-involvement in Kyrgyzstan in 2010 or Tajikistan in 2012.
BORDYUZHA: The CSTO does not get involved in internal conflicts, like the events in Kyrgyzstan in 2010 or in Tajikistan in 2012, because it has been set up to counter external threats. However, the CSTO has had experience of using its troops. If you recall the 1990s, the civil conflict in Tajikistan was resolved with the involvement of Russian military units, peacekeeping forces, border guards, military units from Kazakhstan and Kyrgyzstan, who ensured the security of Tajik borders and, effectively, played a key role in ensuring stability. Also, we conduct military drills every year. Back in 2013, we held six large-scale exercises involving different categories of forces, starting from special-purpose units and on down to troop formations. At these drills, we practice joint combat missions. Of course, we have not yet used our troops in real combat situations, but it is a good thing that so far we have not had to.

SECURITY INDEX: The CSTO does not deal with internal political situations in its member states, but at the same time—going back to the issue of regime change—the extremist social base for this change is formed inside countries. In other words, does it mean that the CSTO will be blocking only militants arriving from elsewhere, while the internal situation will be dealt with by the national governments?

BORDYUZHA: Not quite. Supporters of radical religious organizations advocating extremism in politics should be dealt with by the states themselves, not the CSTO. In this situation, the CSTO must prevent a destabilization of the situation with the use of that section of the population, and must prevent them from being used in breaking up the country, in overthrowing a lawfully elected government. These people must not become a support base for militants trying to infiltrate the country from abroad, as is happening in Syria now and as was the case in Chechnya. Militants cannot come to a stable country where they do not have a social base, as they will not be able to perform their tasks there. They need somebody to rely on. We must prevent a situation whereby outside militants, terrorists, and extremists have a social base inside the CSTO member states.

SECURITY INDEX: Are there plans for expanding the CSTO?

BORDYUZHA: Currently we do not have pending applications to join the CSTO. Furthermore, to join the CSTO, a country must be ready for real cooperation in the very sensitive area that security is. We had an unfortunate experience when Uzbekistan joined the organization but turned out to be unprepared for collective action, unprepared to act jointly in several areas of ensuring security. That is why Tashkent suspended its membership of the CSTO. The thing is that Uzbekistan’s position is based primarily on bilateral contacts and operations in a bilateral rather than collective mode. At the same time, we try to improve CSTO operations through partners. For instance, we cooperate closely with the Shanghai Cooperation Organization and, in particular, with China on a number of security issues. We have close ties with representatives of Iran, and there are more examples of productive contacts with other states.

Thus, we expand our sphere of influence but do it solely in the interests of ensuring our member states’ security, which is our main objective. Having said that, the CSTO does not have claims to a global role.

SECURITY INDEX: In Afghanistan, some 8–10 percent of the population are Uzbeks. How do you propose to interact with them in light of Uzbekistan’s unsuccessful experience of CSTO membership?

BORDYUZHA: Uzbekistan’s position in relation to this situation is a rejection of any collective efforts to contribute to resolving the conflict in Afghanistan. Tashkent relies only on bilateral relations. It was categorically opposed to us providing collective support to the Afghan leadership in ensuring stability, training security, and law-enforcement staff, jointly combating the production and trafficking of drugs. They believe that any efforts should be only bilateral.
SECURITY INDEX: Back in late 2012, the CSTO stood on the threshold of serious organizational reform. Has it been able to carry out everything that was planned? What other changes are to be expected in the near future?

BORDYUZHA: Indeed, in December 2012 the CSTO heads of state agreed to set up additional collective forces, including an air force, a special operations force, and a system of managing these forces. Those decisions were aimed at streamlining military cooperation, making it more effective and, most importantly, building the capability that we will need to counter various threats that we face. Now we are also forming a collective emergency response system. It is a whole set of objectives that will allow us to build our capability for dealing with large-scale natural and man-made disasters.

SECURITY INDEX: Would it not lead to a duplication of functions with the Emergencies Ministry?

BORDYUZHA: No, we seek to develop a system whereby CSTO member states could quickly and effectively render assistance to their partners. That requires systems of monitoring, forecasting, and information exchange as well as the provision of rescue equipment, and joint training. There are many areas for cooperation there.

We are now drafting relevant regulations to cover these areas for cooperation, and will set this system up in 12 to 18 months’ time. For example, we already have an integrated information and software system, the crisis response center. CSTO member states cooperate with each other on a permanent basis and, when necessary, develop joint proposals.

SECURITY INDEX: Does the problem of illegal immigration affect cooperation between CSTO member states?

BORDYUZHA: Of course it does. We have a Coordinating Council of the Heads of the Competent Structures of the CSTO on combating irregular migration. Within that council, we develop joint steps aimed at minimizing those threats and regulating illegal immigration. We are focusing our attention on combating criminal gangs that specialize in the smuggling of migrants and transborder human trafficking.

As for the impact that the known politicization of this issue in Russia has, of course, our partners are not happy with it. One needs to be extremely sensitive here since we are talking about our closest partners, our allies, people who help us ensure our security and who, should it come to this, will be fighting alongside us.

That is why we have developed the foundations of a coordinated information policy inside the CSTO. Under this, member states must undertake to develop friendly ties, to prevent the publication of offensive or humiliating comments regarding their partners. We are not suggesting that objective problems should be hushed up, but we are saying that these problems should be discussed in respectful terms. Besides, we have the Customs Union, which implies free movement of goods, capital, and people. Integration processes in parts of the former Soviet Union continue. We should calm down a bit, take a look at our partners in the CSTO and the CIS as a whole, and realize that they are sovereign states and sovereign nations that should be respected, the same as we respect the Americans or the Europeans. Then everything will be all right.
In the twenty-first century, technology is transforming the world at a tempo that is sometimes too fast for the human mind to grasp, from new types of energy and industries to the unprecedented paradigms of communications. The information technology revolution is proceeding, transforming the landscape of global development and international security. From 3D printing and augmented reality to cyborgization and predictive analytics, digital technology generates new opportunities and new challenges for the world community. Where does this megatrend of digital progress lead humanity? Should we be prepared to adapt familiar social, economic and security processes to the rise of artificial intelligence and the prologue of technological singularity?

Security Index has interviewed Dave Evans, the Chief Futurist at Cisco and Senior Director & Chief Technologist at Cisco Internet Business Solutions Group on the possible implications of the coming convergence of human and computer technology for global development and international security.

SECURITY INDEX: In your forecast Ten Technology Trends That Will Change the World in Ten Years, you claim that advanced technologies for producing solar cells would enable a worldwide transition to solar power. Developing this idea, what do you think of the future of nuclear energy by 2030? Will it survive after Fukushima and other serious incidents and compete successfully with solar power, or is it doomed to decay? What does the future of thermonuclear fusion looks like in 2030—will it become a major means of power generation by that time?

EVANS: Some factors for the future transformation of the world energy market are in place. Today, we already are able to generate an impressive share of energy with solar technologies and nanotechnologies. The solar cell market niche is expanding even with the inefficiencies of existing solar cells, while this technology is continuing to be improved quite rapidly. We are witnessing increasing breakthroughs in solar cells, even including things like organic-based solar cells, where the technology can be recycled as soon as it reaches the end of its lifetime.

As for the perspectives of nuclear power, one of the challenges with nuclear technology today is that it is perceived as being quite dangerous, and some events over the past few years have indicated significant challenges linked with existing nuclear technology. However, if we are able to achieve breakthroughs in nuclear fusion, instead of nuclear fission, things might change dramatically, since fusion promises to be a much cleaner and safer form of nuclear energy. The chances for achieving some fundamental progress in fusion technology seem to be more and more promising every day, although it’s been challenging for some time. So if the day of the breakthrough comes, then the fusion-based nuclear industry has a very optimistic future, and it will certainly give solar a run for its money. However, if we fail to advance the technology and to perform the transition, we will continue to be dependent on nuclear fission, a dirtier type of nuclear power. This scenario, I think, will encourage an increase in renewable energy sources like solar and wind.
SECURITY INDEX: Moving on, I would like to ask a question on 3D printing technologies, which are a specific field of your expertise and kind of your favorite research topic. What are the real perspectives of this technology for the moment and, which is also important, what are its principle limitations, preventing additive production from overthrowing today’s method of industrial production?

EVANS: Already in 2013 about 70 different types of materials could be 3D-printed—everything from ceramics to different types of metals and plastics, and so on. However, one of today’s major challenges for 3D printing is mixing those materials effectively. For example, it is not a problem to print something that is full metal or consists solely of plastic or ceramics. However, a much more challenging task is to 3D-print things that consist of many different types of materials. As you look around your home, a lot of the things that you use consist of a variety of different materials mixed together in a particular device. Let us take your mobile phone as an example—it might have a plastic shell, but it’s also got a glass front, different chemistry inside, perhaps from the battery, electronics, so all in all it is composed of a variety of different materials probably including several hundred of them.

Although 3D printing is very useful for many different types of objects and purposes, it is still not where it needs to be for every type of material. We still lack the solution for effective work with a mix of materials. However, this is going to change—in a number of years we will overcome some of those challenges, and we would be able to print some sophisticated things, including hi-tech electronics like mobile phones; it is just a matter of time.

The real usefulness and demand for 3D printing depends on whether we look at it from a consumer perspective or from an enterprise perspective. Concerning the business perspective, 3D printing is remarkably effective for things like prototyping and for printing parts that are predominantly made out of one type of material like an engine block. In fact, the same is true for the consumer side. One example might be printing some household goods or home furnishings out of ceramics or plastics—quite simple objects in terms of composition, although they can still be complex in terms of geometry and shape. Nevertheless, until we have multiple print heads that can print multiple types of materials and effectively mix them together, no real boost in consumer demand for the 3D printed items and volume of this market would follow.

SECURITY INDEX: What economic and social implications will 3D printing have in a decade from now for the global economy structure, transnational industries and markets? Some of the researchers specialized in small arms predict that the revolution in 3D printing will completely transform the global small arms market and provoke a skyrocketing growth of illegal small arms production and trade. This scenario is potentially applicable to many other industries and many other types of products that are currently produced in a centralized way.

EVANS: Let me address your questions in reverse, because you bring up a very good point on the legal side of things. I too believe that 3D printing will really challenge how we think about intellectual property. For example, let us assume that I design some product and upload it online, and then you download that thing and modify it, augment it or enhance it using your own skills or designer vision. Who owns that original object? Is it you or is it me? As you think about physical objects becoming digital copies of themselves, it starts to bring up questions around property rights management, including the issues of intellectual property. So would I agree on the legal observation.

I do agree that it will also create a lot of what in the USA they call cottage industries, or smaller industries to manufacture products and goods. Perhaps some of them would be legal, while others might actually fall outside the scope of the legal provisions or even directly violate them. Certainly, some cottage industries might conduct activities that perhaps would provoke ethical questions around small arms, or firearms, as you mentioned in your question. Even today, 3D printers can print firearms, including fully functional automated rifles. This raises a variety of questions around access to these capabilities and their legal regulation, which remains largely absent across the globe.

On a positive note, to my mind the flourishing 3D printing would be likely to induce some other very interesting phenomena. For example, it would allow the manufacturing processes
to become significantly virtualized, to allow manufacturing to scale. If 3D printers get to the point where they are sophisticated enough, and at a price point where every consumer can afford one, which is likely to happen in the next 10-15 years, that means that everyone would get the ability to manufacture directly in their home. This completely changes how we think about manufacturing as a hierarchical centralized process with high participation barriers. While the large manufacturing facilities that we have will continue to exist for certain types of products, we will also allow them to scale and virtualize manufacturing, because everyone now has a 3D printer in their home.

3D printing also allows for a massive increase in innovation. Today, if you have an idea for a product, it may be challenging for you to manufacture it, because you need certain industrial facilities and machines to create the product. However, if you were able to simply design it virtually through digital 3D tools and then print that product, the impact of this change on the evolution of the innovation strategies or the entrepreneur strategies for accessing the targeted market could hardly be overestimated. An entrepreneur equipped with the 3D printing facilities could now upload his product design online, and people are able to download it and print the product themselves. In this scheme, no one needs to worry about supply chains, as well as to take care of the large and centralized manufacturing facilities. The technology redefines the criteria and barriers for one to become an innovator and to get one’s product into a global market. I also agree that this technology is potentially a very, very disruptive one—but in a positive way.

**SECURITY INDEX:** My next question focuses on advanced analytic tools known as predictive analytics. For example, there is a company in the United States, Recorded Future, which produces these tools and uses them to analyze Big Data and predict particular events, including typical behavior of selected individuals. Do you share the opinion that such analytic tools may be used in the near future for the practical purposes of business and public administration? Might such predictive instruments find their own niche in the security and strategic management sphere?

**EVANS:** We are definitely going to see a lot more predictive tools of the kind that you are describing, while some of them can be witnessed already. Recorded future is just one example. Recently, I read and tweeted about another company working on the use of Big Data to predict, simply by analyzing four pieces of data with cell phones. The required data input includes the knowledge of where you have been at four different moments throughout a fixed period, and with 90% accuracy they could predict where you are going to be next. This technology is not just about being able to analyze Big Data, it is also about being able to predict human behavior itself. This is obviously important, whether applied for security, retail, or in terms of other applications. A scientist might use such technology to predict where diseases may travel throughout the world. When a flu epidemic broke out a few years ago, Google Maps were used to illustrate where the virus might travel and be disseminated. Today this technology, which has become even more sophisticated, might be adapted for tracing the dissemination of the Ebola virus or other similar diseases.

Being able to mine all this massive amount of data that all users are creating, whether on social networking sites like Facebook, or Twitter, even on YouTube, or the data inside an enterprise, the information society is starting to follow a simple rule. The more data we have, the more we can make intelligent forecasts based on it. Things like an organization’s ability to forecast supply chain fluctuations based on looking at recent historical trends and actions and customer behavior would turn into a common practice in a quite foreseeable perspective. As far as I suppose, we will be able to predict the outcome of events before they happen, including stock market fluctuations before they occur, and the outcome of elections before the final vote is cast. And this ability obviously is going to be a very powerful tool, even with regard to possible outcomes of accidental miscalculations, let alone purposeful manipulations with the predictive tools.

I would also reference quite a bit the work that IBM has been doing with the Watson supercomputer. This is an important tool because it can process massive amounts of data very rapidly—I believe its capacity is 60 million pages of content per second. Moreover, not only can Watson absorb this data, but it can understand information, even that which people cannot process. It is claimed to understand language, to understand metaphors and similes,
and to understand the subtleties of speech and language. Watson is able to take those data and process them in a way similar to how a human brain processes language, so it can make inferences between different things in the content. So as we start to take the data analytics in some of the work like what Recorded Future is doing and couple it with some of the work IBM is doing with machines like Watson, and add to it this massive amount of data that is produced in the information society, I suppose at the outcome we get tools enabling anyone who effectively possesses and uses them to become a futurist, with a whole ambivalent spectrum of consequences.

SECURITY INDEX: Today, we are witnessing the rapid development of biotechnologies and their mounting convergence with advancements in ICT, which lead to the technology that is often referred to as cyborgization. Do you believe that by 2030 cyborgs will turn into a widespread technology and become available to the average market consumer in developed countries? If the reply were positive, then which segments of the global market would this technology saturate, and what occupations and segments of the labor division would generate most demand for it? Would the proliferation of cyborgs involve particular implications for international security?

EVANS: In a certain way, production of cyborgs is already a widespread technology that everyone uses, just in a very simplistic way. For example, when you put on eyeglasses, you are enhancing your ability to see. When you wear hearing aids, you are enhancing your ability to hear, and when you use a mobile phone, you are advancing your ability, though arguably, to practice telepathy over the network, because you are not actually speaking to that person live, but communicating with a digital representation of that person’s voice. We already use the cyborgization technology to extend who we are, to reach out to any other person on the planet.

Today, most of this technology is outside the human body, so basically it is something that we wear. But in the coming decades, certainly in the 2030 timeframe, a lot of this technology will be embedded in humans’ bodies because it will get small enough to be easily implanted inside of us. Today we are starting to witness the development of devices like exoskeletons. People that were born paralyzed are now able to walk again through the aid of sophisticated exoskeletons. As an example from a different field, using an exoskeleton in a combat situation, you can run faster or carry a lot more weight than a human normally could.

Major advances also take place in devices like brain–machine interfaces that allow people to control a prosthesis, an exoskeleton, any other external device by thinking about doing it. In all of these examples, the technology tends to be integrated into who we are. An increasing diversity of these “cyber-type” capabilities are emerging around us and inside us. Selected examples include brain–machine interfaces, exoskeletons, 3D printing of human organs, artificial retinas enabling people who were blind to regain their eyesight, artificial cochleas bringing back to people who were born deaf the ability to hear. To sum up, the process of integration of technology into biology has already begun. Within the 2030 timeframe, I suppose we would think nothing of seeing humans augmented by technology. Sometimes the technology will be deeply embedded in the human body; sometimes it will be visible and external. However, the very phenomenon of merging of man and machine will continue to evolve and expand in terms of both sophistication and popularity, just because it does allow us to enhance who we are.

At the same time, I do not think that it is going to become specific or focused around any particular industry; instead, the technological trend will develop across all industries. Of course, in terms of military applications, humans will certainly be augmented. But a huge potential demand also exists for medical applications; thus, a surgeon may be augmented with special visual capabilities enabling him to see what he is working on with higher clarity. Going even further, a surgeon might have tools integrated into his body that would allow him to perform surgery with a dexterity unmatched for an ordinary human. So the process could hardly be limited to any single market or industry niche; on the contrary, we are going to see a merging of the technology and biology industries and new niches emerging in this technology-augmented environment of human activities and operations.
SECURITY INDEX: In your previous passage, you mentioned brain-machine interfaces; I have another question that is closely related to this concept. As technologies conform to the global nature of human communication, the global network—the Internet—also continues to transform itself. As far as might be deduced from your forecast and from the observations of other prominent futurists, in 15 or 20 years from now the Internet as we know it today could completely change to something very different, including shifts on the infrastructure level. What emerges instead might be a global network of communications on a completely different technological basis, even based on new physical principles. There are some expectations that this new type of network, which could substitute or devour today’s Internet, would be even more net-centric, less centralized, and practically omnipresent. Due to these qualities, it would be practically impossible to subordinate it to any sort of centralized hierarchal control, including any sort of governmental control. Do you agree with that, and how do you see the future of the Internet in the infrastructural sense? What technology might constitute the core of the network of the future?

EVANS: I do generally agree with that premise. What we are doing is creating a digital nervous system for the planet, and we see a few trends occurring. First, more and more objects are getting connected, billions of devices are linked through the global network—and according to Cisco there might be over 50 billion devices online in the next decade. Those devices are not just the traditional objects that we are used to seeing connected, not just computers, laptops, mobile phones, etc. The Internet of Things enables online connection for objects like a house, a car, one’s clothing and medical devices, and even a farmer’s livestock. Of course, such types of objects are getting connected not by themselves but due to the work of computer devices integrated in their construction or lifecycle.

Second, these devices are starting to sense, because the researchers and market pioneers are adding smart computer sensors to the objects that constitute our world at a rate that never took place before. We are literally getting visibility into climate changes, temperature, reallocations of people, movement of supplies and goods, the environment, and so on. We are sensing our world in completely different ways now because of the ICT-enabled augmentation of sensor capabilities.

We are also adding very sophisticated computing devices to the networks. We talked about IBM’s Watson supercomputer as one example, but as you follow Moore’s Law over the next couple of decades, it means that computers will be billions of times more powerful and faster than they are today. As you put billions of these computers, which are now billions of times faster, onto the network, this network is going to consist not only of things that can sense.

That would include things that can arguably think or make decisions, whether the outcome would be full-fledged artificial intelligence or just some extremely sophisticated self-learning scripts. Just by putting together endless resources of numerous advanced computer devices, we would make a huge step towards creating an omnipresence of thinking, a global environment of sensing infrastructure. One of the promising technologies that researchers are working on is this notion of a quantum network. Some advances in quantum routing are already almost in place, e.g. the ability to exploit things like quantum entanglement, to use that to send information across the network in secure, encrypted ways. Potentially we might even be able to use this technology at some point to create unbelievably fast networks.

So in total, if you start adding together all the technologies enumerated above—the ability to sense, billions of connected smart devices, nontraditional devices that are now sensing and communicating, coupled with machine learning and intelligence, coupled with an increase in raw connectivity, quantum entanglement, exploitation, or new types of wireless technologies, etc., the outcome you might likely come to is that in a couple of decades from now, the network indeed is going to look entirely different than it does today.

SECURITY INDEX: So, in 20 years there would be neither DNS servers or domain names as such, nor IP addressing and all those infrastructure layers of today’s Internet?

EVANS: I do not mean that there would not be anything like that, because we still need a reliable way to connect the network nodes and to uniquely identify objects and devices in the
global computer networks. However, some totally new technological solutions might emerge instead of the DNS system and IP addresses as we know them today. Consider, for example, that back in the early 1990s, we had many different protocols for crawling across the network. We had Apple Talk and Token Ring and IP as parallel or even competing solutions; and eventually, we standardized on IP as the dominant technology. Today Internet users are migrating from IP version 4 (IPv4) to IP version 6 (IPv6), which is another major transition. When it is complete, in the next few decades we may start transition to some other innovative realization of the Internet’s unique identifiers idea. It may be based on IP; with equal chances it might be based on something completely different from the present-day system of IP-addressing. It might be a fair conclusion to say that things will still be uniquely addressable, because what seems to be evident is that the demand for real-time ICT-enabled connection between nodes, networks, and communities would only increase, so the unique identification procedures would still constitute a basis for that.

Whether or not we have DNS as it stands today, we still need some way to translate between how a human understands something and how a machine understands and interprets it. When you go to the http://google.com website as a user, it is convenient for you to remember the domain name “google.com,” but the hardware and software constituting the Internet’s infrastructure does not know what this domain is, because it looks up the IP address on a lower infrastructural layer. So we will still need that kind of translation between machine and human, even if the distinction will not be linked to the DNS and other layers of today’s network infrastructure.

SECURITY INDEX: By 2030, the sum of advanced information technologies, and in particular the Internet, will probably make the human more self-efficient and independent in his economic anthropogenic activities, social communication, healthcare, etc. As a result, he may become distinctively more autonomous and independent in satisfying his needs. Will this fundamental ICT-induced change induced by technology trigger further transformation in the social architecture of human society? Would traditional nation-states, which are inherently based on hierarchical structures, centralization of production, economic activities, security, and social welfare, etc., ever survive these shifts? What social structures are going to emerge instead of nation-states as manifestations of a new self-sufficient individual, feeling no vital need for centralized governance?

EVANS: It is fundamentally difficult to predict human behavior. Just look at how the global network has already changed our behavioral patterns in astonishingly multiple ways. Think of its impact on the way we communicate with one another, the way we have empathy for one another, how we think about healthcare and education differently; the information technology revolution has been already changing some of the basic and peripheral social norms, and that process will go on. In this regard it is important to stress that one of the most fundamental things that connectivity does is to provide increased quality and transparency. Government and individuals can no longer hide behind anonymity, because the network now allows for transparency.

It also allows for equality, because people who did not have access to something like healthcare or education now start to enjoy it because of ICT-enabled connectivity. There was a great story in 2013 on very innovative work that Microsoft and Google were doing in some towns in Kenya. Using solar technology and the white space in television signals, they brought 60 Mbps broadband connectivity to local towns that previously had no access even to electricity. This means that individuals in those communities in fact were granted access to healthcare, education, and information they need to make decisions and structure their life and activities more efficiently.

Still, it is unclear to me how the human dynamic will change exactly; but based on what is evidenced so far, I have little question in my mind that we will continue to evolve to the benefit of transparency-based practices and norms. We will continue to have greater empathy for one another, and greater visibility, and enhanced and improved access to information and resources, greater ability to share with one another. I think that if anything, what this does is bringing us much closer together as a species, as a population of a global planet, because we can now share, sense, and communicate in ways that were impossible in the historic past of the humankind.
SECURITY INDEX: My last question is on technological singularity. When anyone starts to speculate on technological singularity, there are two unclear issues. First, is there anything beyond the point of singularity? Does everything stop or turn into some unknown condition of absolute knowledge, and is there any further development beyond that point? Second, should technological singularity be described and considered in positive or negative terms? Is there any scenario of positive technological singularity, which would empower the realm of absolute knowledge, unlimited progress, and social transparency? Conversely, what might the negative scenario look like? Could it correspond with the popular sci-fi narrative about creation of some artificial hyper-intelligence, which confronts and eventually suppresses its human inventors—or, much more trivially, would the human mind just collapse under the huge amount of data?

EVANS: One thing that is underestimated when people talk about singularity is its non-technology implications. There are cultural, philosophical, religious, political, and other considerations. Those are things that will take some time to figure out, but purely from a technology perspective, there is no reason that would irrevocably prevent humanity from arriving at technological singularity. If you look at Moore’s Law and some other rules like the Law of Accelerating Returns, it looks like within the next three or four decades we will hit that threshold.

When trying to analyze the possible implications of singularity and describe them as positive or negative, we need to stress that in the first iteration that would mean less of a machine versus man—and more of a man and machine merging. Humanity will continue to augment itself with technology. It may be biologically inspired technology—quite like the recent case when Stanford University scientists created a biological transistor using RNA and DNA of a living being. When we speak about augmenting ourselves with technology, it may not be silicon-based technology; it could, rather, be technology using our own biological potential to enhance who we are. What I would like to stress is that in a long-term perspective this kind of convergence appears to be an inevitability.

What follows after? This is really getting beyond the forecasting horizon, but do not forget that the Earth is just one small planet in the Solar System with billions, or arguably hundreds of billions and possibly trillions of planets in the Universe. Even if we ourselves witness the advent of singularity in the next few decades, there is so much potential to explore the stars. We have not even set foot on another planet yet—even on Mars—and that is the next logical step. I think what is going to happen as we approach and pass technological singularity is that humanity as a species will continue to expand who we are and where we are.

The time we start reaching out into the stars and traveling past our own Solar System may be about 200 years from now. The technology that we need to travel faster than light through the manipulation of space–time warping we may not have for another century or two. But there is plenty for humans to discover and learn once we are no longer constrained by the planet that we currently inhabit. So, if singularity comes to pass, that is not the end—that would be really just the beginning of where the human species is going to.
In terms of its portfolio of contracts and actual deliveries, Russia has for a long time been the world’s second-largest arms supplier after the United States. Over the past few years Asia Pacific has been the biggest destination of Russian arms exports, accounting for 55—57 percent of the overall figure. The Middle East is second with 14.2 percent, followed by northern and northeastern Africa with 12.7 percent. The top ten of the largest buyers of Russian weaponry in these two regions includes Algeria; Iran (4.1 percent of total Russian exports), Syria (3.1 percent), Egypt (3 percent) and the UAE (1.8 percent).

In 2012 Russia exported about 15.2 billion dollars’ worth of weapons, of which the Middle East accounted for about 20 percent. But of all the Middle Eastern countries, only Iraq made it into the Top 10 of the biggest destinations of Russian defense exports in 2012. That year, the country placed 4.2 billion dollars’ worth of tentative orders for Russian weaponry, which accounts for 23.17 percent of the defense contracts Russia signed in 2012.

But the ongoing military and political developments in the Middle East and North Africa are putting growing pressure on the regional balance of Russia’s defense exports. It has already become clear that the share of Middle Eastern countries in these exports is sliding. This has already been recognized by Russian officials. Let us therefore look more closely at this situation in order to identify its possible consequences.

THE GULF MONARCHIES: STRANGERS ARE NOT WELCOME

BAHRAIN

Bahrain maintains close military-political ties with Washington. The country hosts the headquarters of the U.S. 5th Fleet, and buys weapons mainly from the United States. Bahrain’s oil reserves, and therefore its revenues from oil exports, are limited. For that reason, the country often buys or leases used weaponry in an effort to cut costs.

In recent years Bahrain has ranked 57th among the world’s largest arms importers, and 13th in the Middle East, just ahead of Yemen and Lebanon (not counting the Palestinian Autonomy), with a 0.7-percent share of the region’s arms imports.

Military and technical cooperation between Russia and Bahrain is almost nonexistent. The only known weapons deal between the two countries was a single delivery of 40 KAMAZ-4326 trucks in 2004. Some small orders may also have been placed for weapons used by special task forces (there is no official information concerning such contracts). So far, that is about it in terms of the Russian presence on Bahrain’s defense market. There were intense negotiations between the two countries about possible aircraft contracts during the Bahrain International Airshow in 2010—but they do not seem to have yielded any results.

Given the utter dominance of the United States in Bahrain’s defense market, Russia is unlikely to win a significant share of that market any time soon. There is a small chance of
Bahraini contracts for Russian military-transport helicopters, combat trainer aircraft, and ground weaponry. But these contracts may materialize only in a fairly distant future, if at all.

**QATAR**

This emirate pursues a pro-Western course, and has come under the very strong influence of the United States. Qatar also hosts a large U.S. military base, which clearly affects the country’s choices in terms of what kind of weaponry it buys, and from whom. France used to have fairly strong positions in the Qatari defense market, but in the past decade that market has been dominated by the United States.

Over the past eight years Qatar has ranked 12th among the largest Middle Eastern weapons importers. In dollar figures, it is fairly close to Iran; by 2015 Qatar will have spent an estimated 1.186 billion dollars on arms imports. The United States will account for 750 million dollars (63.2 percent), followed by Germany and Switzerland with 150 million dollars apiece (12.65 percent). Qatar has also signed small-arms contracts with Italian, French, and Dutch suppliers.

There is very little arms trade between Russia and Qatar. The only known deal is the single sale of 500 KAMAZ army trucks in 2004, and no major breakthrough is expected any time soon. The best Russia can hope for is small programs related to the repairs of previously supplied hardware, and/or orders for small batches of armored vehicles or dual-use products.

Russia and Qatar are also negotiating contracts for certain weapons systems used by special task forces (in fact, some contracts may have already been signed). But any significant increase in arms trade between the two countries is highly unlikely. The reasons for this include Qatar’s strongly pro-Western orientation. Also, supported by the Americans, Qatar is strengthening its position as Russia’s main competitor in the market for natural gas. Moscow has already lost a share of the European energy markets to the Qatars.

**KUWAIT**

Even though Kuwait is a typical pro-Western Arab monarchy, it tries to maintain friendly relations with many other countries, including Russia. Kuwait has largely competed the restoration and modernization of its armed forces after the Iraqi occupation of 1990–1991. It has been buying weapons not only from the West, but from Russia as well (including BMP-2 and BMP-3 infantry fighting vehicles and Smerch MLR systems). Nevertheless, the Kuwaiti defense market is dominated by the United States, and this situation is unlikely to change any time soon.

Russia is now trying to get the Kuwaitis interested in its upgrade options for the M-84AB and BMP-3 armor, as well as in Russian air defense systems. But the country has not placed any large orders for Russian weapons since 2002, with the exception of a 2009 contract for two Project 12061E Murena amphibious assault hovercraft. The deal was signed to offset part of the Russian debt to Kuwait, but as of autumn 2013 no information was available on the progress made on this particular contract. Also, Russia is about to complete an upgrade project for Smerch MLR systems previously supplied to Kuwait, and has begun to upgrade the Kuwaiti fleet of BMP-3 infantry fighting vehicles.

In the medium term, any significant increase in arms trade between Russia and Kuwait is unlikely, although the Kuwaiti armed forces could place up to 100 million dollars' worth of small contracts by 2015, mostly for the repair of previously supplied weaponry.

**UAE**

The United Arab Emirates is one of the Arab world’s richest countries. Its defense spending has been growing steadily in recent years. It is the second-biggest arms importer in the Middle East after Saudi Arabia. The UAE has always pursued a policy of diversification of its arms imports; nevertheless, its defense market is dominated by U.S. suppliers.

One of the largest weapons deals in history was the 2007 contract between the UAE and the United States for nine PAC-3 SAM batteries, worth 9 billion dollars. In 2008–2011 U.S.
Bahraini contracts for Russian military-transport helicopters, combat trainer aircraft, and ground weaponry. But these contracts may materialize only in a fairly distant future, if at all.

**QATAR**

This emirate pursues a pro-Western course, and has come under the very strong influence of the United States. Qatar also hosts a large U.S. military base, which clearly affects the country’s choices in terms of what kind of weaponry it buys, and from whom. France used to have fairly strong positions in the Qatari defense market, but in the past decade that market has been dominated by the United States.

Over the past eight years Qatar has ranked 12th among the largest Middle Eastern weapons importers. In dollar figures, it is fairly close to Iran; by 2015 Qatar will have spent an estimated 1.186 billion dollars on arms imports. The United States will account for 750 million dollars (63.2 percent), followed by Germany and Switzerland with 150 million dollars apiece (12.65 percent). Qatar has also signed small-arms contracts with Italian, French, and Dutch suppliers.

There is very little arms trade between Russia and Qatar. The only known deal is the single sale of 500 KAMAZ army trucks in 2004, and no major breakthrough is expected any time soon. The best Russia can hope for is small programs related to the repairs of previously supplied hardware, and/or orders for small batches of armored vehicles or dual-use products.

Russia and Qatar are also negotiating contracts for certain weapons systems used by special task forces (in fact, some contracts may have already been signed). But any significant increase in arms trade between the two countries is highly unlikely. The reasons for this include Qatar’s strongly pro-Western orientation. Also, supported by the Americans, Qatar is strengthening its position as Russia’s main competitor in the market for natural gas. Moscow has already lost a share of the European energy markets to the Qataris.

**KUWAIT**

Even though Kuwait is a typical pro-Western Arab monarchy, it tries to maintain friendly relations with many other countries, including Russia. Kuwait has largely competed the restoration and modernization of its armed forces after the Iraqi occupation of 1990–1991. It has been buying weapons not only from the West, but from Russia as well (including BMP-2 and BMP-3 infantry fighting vehicles and Smerch MLR systems). Nevertheless, the Kuwaiti defense market is dominated by the United States, and this situation is unlikely to change any time soon.

Russia is now trying to get the Kuwaitis interested in its upgrade options for the M-84AB and BMP-3 armor, as well as in Russian air defense systems. But the country has not placed any large orders for Russian weapons since 2002, with the exception of a 2009 contract for two Project 12061E Murena amphibious assault hovercraft. The deal was signed to offset part of the Russian debt to Kuwait, but as of autumn 2013 no information was available on the progress made on this particular contract. Also, Russia is about to complete an upgrade project for Smerch MLR systems previously supplied to Kuwait, and has begun to upgrade the Kuwaiti fleet of BMP-3 infantry fighting vehicles.

In the medium term, any significant increase in arms trade between Russia and Kuwait is unlikely, although the Kuwaiti armed forces could place up to 100 million dollars' worth of small contracts by 2015, mostly for the repair of previously supplied weaponry.

**UAE**

The United Arab Emirates is one of the Arab world’s richest countries. Its defense spending has been growing steadily in recent years. It is the second-biggest arms importer in the Middle East after Saudi Arabia. The UAE has always pursued a policy of diversification of its arms imports; nevertheless, its defense market is dominated by U.S. suppliers.

One of the largest weapons deals in history was the 2007 contract between the UAE and the United States for nine PAC-3 SAM batteries, worth 9 billion dollars. In 2008–2011 U.S.
weapons deliveries to the country reached an estimated 7.335 billion dollars, which makes up 66.1 percent of UAE weapons imports over that period (11.095 billion dollars). Russia was a distant second with 891 million dollars’ worth of arms deliveries to the UAE, followed by France (818 million), Germany (507 million), and Switzerland (307 million).

The United States is expected to retain its huge share of the UAE defense market over the coming years. Its accumulated arms deliveries to the country are expected to reach 12.717 billion dollars by 2015, which makes up 77.53 percent of the total figure. France is expected to make another 1.881 billion dollars’ worth of deliveries, followed by Italy (607 million), Switzerland (204 million), and Sweden (180 million). Russia is not on the list of the biggest arms suppliers to the UAE.14

Nevertheless, arms trade between Russia and the UAE has a long history. Since the early 1990s Russia has supplied large batches of armored vehicles (815 BMP-3 infantry fighting vehicles and other armor using the BMP-3 chassis), as well as Smerch MLR systems, Igla and Igla-S man-portable SAM systems, anti-tank and anti-aircraft missile systems, and trucks. But in 2001 Russian arms deliveries to the UAE began to fall. The only large contract in recent years was for 50 Pantsir-S1 gun-missile AA systems; the development of that product was commissioned by Abu Dhabi. The deal was worth 734 million dollars.

Russia and the UAE have long been in talks about a possible contract to develop an integrated air defense system for the Arab state based on the Russian S-400 SAM system. So far, however, these talks have not yielded any results, even though a proposal was made in 2007 about in-kind repayment of Russian debt to the UAE by weapons supplies.15 In the 2008–2011 period Russia supplied 890.6 million dollars’ worth of weaponry to Abu Dhabi, but since then deliveries have fallen sharply.16

So far, the possibility of Russia winning a significantly larger share of the UAE defense market appears remote. In 2013 Rosoboronexport completed a 75.2 million-dollar upgrade project for 135 previously supplied BMP-3 vehicles,17 and the Tula-based Instrument Design Bureau (KBP) signed a 128.63 million-dollar contract for various types of ammunition.18

OMAN

The Sultanate of Oman is one of the most militarized states in the Middle East. Thanks to its oil export revenues, the country has taken its military spending to record levels. Oman does not have a clearly demarcated border with its neighbors, so tensions flare up from time to time with the UAE, Saudi Arabia, and Yemen.

The main arms suppliers to Oman are Britain and the United States. In recent years, defense contracts were also signed with France, Germany, South Africa, Pakistan, India, Jordan, and Saudi Arabia. In 2003–2009 Oman received almost 1 billion dollars’ worth of American weaponry. The country’s territory remains a key base for the Western countries in the event of military action in the Middle East. That is why the Americans and the British treat Oman differently from many other Arab countries, to which they usually sell obsolete weaponry; Oman receives fairly advanced and up-to-date military hardware.19

Arms contracts between Russia and Oman have been few and far between. In fact, the only known contracts are the 1992 sale of six T-80 tanks (according to the UN Conventional Arms Register), and the 2005 order for a batch of 9K129 Kornet-E anti-tank missile systems.20 Oman has also expressed interest in the Russian-made Bastion coastal defense missile system, which is equipped with PG-10 BrahMos supersonic anti-ship missiles (developed jointly by Russia and India).21 But there has been no information about an actual contract being signed for that weapons system.

On the whole, Russia is making efforts to revitalize its arms trade with Oman22, but with little to show for it so far.

SAUDI ARABIA

Saudi Arabia plays an extremely important role in the current system of global and regional international affairs. Its historical background and role as the guardian of the holiest Muslim
places have made the country the global center of Islam, which largely determines its foreign policy course, and its aspiration for leadership of the Muslim world. Being the largest oil producer in the Middle East, and a key U.S. ally, Saudi Arabia spends huge amounts of money on weapons. On the one hand, Washington supplies the Saudis with the latest defense hardware. But on the other, it tries not to undermine Israel’s regional superiority in defense technology.

A new wave of Saudi defense contracts began in 2006, when the country placed about 13 billion dollars’ worth of orders for American and French weaponry. That is about as much as the country had spent on these purposes during the entire period 1998–2005. In 2007 Riyadh also signed a large contract with Britain for 72 Eurofighter Typhoon aircraft worth 8.9 billion dollars (the overall value of the deal could well top 20 billion dollars). The Saudis are currently negotiating other large contracts for aircraft with Britain and France. They are also expected to place orders for tanks, air defense systems, and escort ships.

Britain is currently the biggest arms supplier to Saudi Arabia, followed by the United States (3.417 billion dollars), France (880 million), Canada (498 million), and Turkey (408 million). A total of 11 countries have been selling weapons to the Saudis in recent years; Russia is not among them. In terms of the overall value of arms supplies to Saudi Arabia by 2015, the United States is expected to top the ranking with 16.843 billion dollars’ worth of exports.

Russia has long been trying to win a share of the Saudi defense market, but with little to show for these efforts. It is known that the Russian T-90S main battle tank has undergone trials in Saudi Arabia. At one point the two countries were negotiating contracts for various types of armor worth about 1 billion dollars. The Saudis have also shown interest in Russian air defense systems and helicopters.

In the summer of 2009 Russia and Saudi Arabia signed a framework agreement on military and technical cooperation. Since then there have been several reports claiming that Moscow and Riyadh are negotiating a package of contracts for Russian helicopters, air defense systems, and armor worth more than 4 billion dollars. There have not been any reports about an agreement being reached—but it has not been reported that the talks have ended, either.

On the whole, the Saudi Arabian weapons market remains off limits to Russia. What is more, there has been a notable rise in tensions between the two countries since 2012 due to the events of the Arab Spring, and especially in connection with the crisis in Syria.

THE ARAB SPRING AS A MARKET FACTOR

EGYPT

Egypt buys most of its weapons from Western countries, especially the United States. The arms trade between Egypt and Russia fell sharply in 1972; only a handful of small contracts have been signed since then. In the period since 1990 Egypt has bought a batch of Mi-17 helicopters and various spare parts for Soviet-made weaponry. Most of the recent sales are in such categories as SAM systems and air defense weaponry, as well as upgrades of previously supplied air defense systems. The bulk of the Russian defense exports to Egypt currently consist of several hundred Iгла-S man-portable SAM systems. No contracts have actually been cancelled in the wake of the Arab Spring, but the deadlines have been pushed back. Sales have been particularly slow since 2012, and the total value of contracts signed is expected to reach only 343.3 million dollars by 2015.

Egypt needs to refresh its fleet of combat aircraft, but for now the United States is refusing to sell the latest versions of the F-16 to the Egyptians. There is, therefore, a chance that Cairo will turn to other suppliers of advanced fighter jets, including Russia. Nevertheless, the Russian—Egyptian arms trade is more likely to remain limited to air defense systems and helicopters.

YEMEN

There is much domestic instability in Yemen due to ongoing tensions between the north and the south of the country, rivalry between its numerous tribal groups, and the activity
of Islamist extremists. In the foreign-policy arena, Yemen has major differences with Saudi Arabia and Eritrea. The country has been a Russian defense customer since Soviet times.\textsuperscript{30}

In 1998 Russia and Yemen signed an agreement on military and technical cooperation. Yemeni imports from Russia have included 31 T-72B main battle tanks; 16 MiG-29 fighters, which were upgraded in 2003–2005 to the MiG-29SMT specification; six new MiG-29SMT jets; 11 Mi-171Sh helicopters; several civilian helicopters; and significant numbers of infantry fighting vehicles, small arms, and various types of ammunition. Russia has also upgraded and conducted a technical inspection of 80 Soviet-made Tochka tactical missile systems. At one point Yemen was planning to place up to 1.3 billion dollars' worth of new orders for Russian weapons,\textsuperscript{31} but the Arab Spring has derailed those plans. Accumulated Russian arms exports to Yemen reached 363 million dollars in 2011.

There is a chance of Yemen placing more weapons orders with Russian suppliers if the domestic political situation in the country returns to normality—but these orders are unlikely to be big. The reasons for that include not only Yemen’s financial constraints, but also the growing military-political influence of the United States, which has been donating helicopters, patrol boats, and trucks to Yemen, as well as training Yemeni soldiers free of charge.\textsuperscript{32}

Judging from the information available about the meeting in April 2013 between Russian Prime Minister Dmitry Medvedev and Yemeni President Abd Rabbuh Mansur Hadi,\textsuperscript{33} Yemen is primarily interested in small arms and ammunition, which can be supplied very quickly from Russian weapons depots, as well as engines for previously supplied armor.

**SYRIA**

Syrian President Bashar Assad is trying to preserve his authoritarian Ba’athist regime, but his efforts are looking increasingly desperate. For a long time, confrontation with Israel over the Golan Heights remained at the core of Syrian foreign policy. Essentially, a state of undeclared war continues to exist between Syria and Israel, as witnessed by regular Israeli airstrikes against Syrian targets. At the same time, the ongoing civil war in Syria has become a major headache for the international community. So far, all attempts to get the Syrian government and the opposition to negotiate have failed.\textsuperscript{34}

Despite the difficult military-political situation in and around Syria, military and technical cooperation between that country and Russia continues. Until 1991 Syria was the largest foreign recipient of Soviet weaponry. A new stage of Russian–Syrian military and technical cooperation began in 1998. Since then, Russia has supplied the Syrians with the Metis-M and Kornet-E anti-tank missile systems; Igla MANPAD systems; Strelets turrets; guided tank projectiles; RPG-29 grenade launchers; and other weapons. Contracts have also been signed for the Buk-2ME, S-300PMU-1, and Tor-M1 SAM systems, as well as MiG-29 fighters. In 2010 Russia made final deliveries under a Syrian contract for 36 Pantsir-S1 gun-missile air defense systems.

Negotiations are ongoing on a number of potential contracts, including orders for two diesel-electric submarines, large batches of MiG-29SMT and Yak-130UBC fighters,\textsuperscript{35} and upgrades of the S-125 Neva SAM system. Also, Russia is still considering the possibility of supplying and/or upgrading helicopters,\textsuperscript{36} heavy armor, tactical missiles, various types of combat ships, and other weapons.

Russia continues to fulfill Syrian contracts for 24 MiG-29M/M2 and 36 Yak-130UBC fighters, but making actual deliveries is extremely difficult owing to what amounts to a blockade of transport routes into Syria by Western countries.\textsuperscript{37} In 2008-2011 Russia supplied 1.49 billion dollars worth of weapons to Syria. By 2015 it is expected to make another 2.24 billion dollars’ worth of deliveries, barring any force-majeure circumstances.\textsuperscript{38}

Amid the ongoing civil war, the United States and several other Western countries want Russia to stop its arms supplies to Syria,\textsuperscript{39} but the government in Moscow has taken an unyielding stance on this issue. It argues that since there are no UN sanctions in effect against Syria, there are no reasons to stop military and technical cooperation with that country.\textsuperscript{40}
ISRAEL AND ITS NEIGHBORS: THE PRICE AND VALUE OF A DELICATE APPROACH

ISRAEL

Russia is an importer of Israeli weaponry. The first weapons systems Russia bought from Israel were unmanned aerial vehicles (UAVs). In June 2009 it placed orders for 12 Bird-Eye 400, I-View MK150, and Searcher Mk II drones, worth a total of 53 million dollars. It later placed a 100 million-dollar order for another 36 drones.

The next step was the signing in September 2010 of the first-ever military cooperation agreement between the two countries. This was a framework document that facilitates the signing of new contracts. Moscow hoped that one of these future contracts would be for a joint UAV production facility in Russia. Later that year Israel Aerospace Industries and Oboronprom signed a contract to build a new facility that would assemble Israeli drones in Tatarstan. But the deal has stalled due to Russia's energetic military and technical cooperation with Iran (prior to the introduction of the UN Security Council embargo) and Syria. Discussions between Russia and Israel about building the joint UAV facility have not been broken off completely, but nor is major progress being made.

Nevertheless, the Russian order placed for Israeli UAVs has played a positive role, and stimulated the development of similar systems by Russia's own defense industry. This is especially important because Israel had no plans to transfer the underlying UAV technologies to Russia.41

JORDAN

Russia attaches great importance to cooperation with Jordan in all areas (military and technical, economic, political, etc.) because the country lies at the very heart of the region. Since the mid-2000s Moscow has given Amman a 350 million-dollar loan for the purchase of Kornet-E anti-tank missile systems, Iгла-S MANPAD systems, and several II-76MF aircraft. Russia's Oboronprom and the King Abdulla II Design Bureau have signed a contract for six Ka-226 light multirole helicopters. The contract also includes the establishment of a joint venture that will make helicopter components.

The most important Russian–Jordanian weapons deal was the 2008 agreement on the construction of a new plant in Jordan to make RPG-32 Hashim anti-tank grenade launchers.42 The plant was launched in 2013; it was expected to produce 20,000 grenade launchers by the end of 2013 and reach the capacity of 60,000 launchers in a few years.43

For all these Russian achievements, however, most of the weaponry Jordan receives is used American, British, and other Western hardware; the bulk of it is donated as military aid. Before the Arab Spring the United States controlled a lion's share of the Jordanian defense market. In 2008–2011 it supplied 1.363 billion dollars' worth of weapons, which is 65.5 percent of total Jordanian weapons imports. The United States was followed by Russia (175 million dollars, 8.4 percent), and Belgium (173.7 million dollars, 8.35 percent). Other suppliers included China, the Netherlands, Turkey, South Africa, Ukraine, Britain, the Czech Republic, and Austria. If things go well, Russia will retain its current positions in the 2015–2016 time frame, although its accumulated exports will reach a relatively modest 120 million dollars by 2015.44

LEBANON

This a relatively advanced country, but it suffers from extreme internal instability, always teetering on the brink of civil war between its various religious and ethnic factions. The Lebanese army has long been used mostly as a domestic political instrument, and it cannot afford to buy modern weaponry. Most of its hardware is used American weapons received free of charge as military aid. Western countries have strong reservations about supplying weapons to Lebanon. Nevertheless, apart from the United States, the list of ground and naval weapons exporters to that country includes France, Germany, Italy, and some Arab states (the UAE, Jordan and, prior to the Arab Spring, Libya).45

On several occasions groups of Lebanese officers were trained in Russia, but there is little military and technical cooperation between the two countries. There have been several
reports since late 2008 claiming that Russia plans to transfer 10 used MiG-29 fighters to Lebanon free of charge, and to train Lebanese pilots.\textsuperscript{46} Beirut has also shown interest in Russian armor, artillery systems, and helicopters. The Lebanese were hoping, however, that these future imports would be financed by Saudi Arabia and the UAE, or by a low-interest Russian loan.

The problem is that Lebanon cannot put fighter jets to good use anyway because the country lacks the infrastructure to maintain them; neither does it have the required numbers of qualified technicians and pilots. For that reason, Moscow and Beirut were at one point discussing the possibility of supplying 10 Mi-24 attack helicopters instead of fighter jets; these discussions do not appear to have been broken off completely. During the latest meeting between the two countries’ presidents in January 2013, they stressed the importance of all areas of mutual cooperation, including military and technical cooperation.\textsuperscript{47} On the whole, it is safe to say that Russian arms trade with Lebanon is in a nascent state, and no major progress is expected any time soon.

\textbf{THE PALESTINIAN AUTONOMY}

The Palestinian Autonomy receives weapons through legitimate imports (from some Arab states) as well as smuggling. There are no official figures about the PA’s military spending, and no reliable data are available about its defense procurement. In 2008 it was officially reported that Russia had agreed to transfer two Mi-17 military transport helicopters and about 50 armored personnel carriers to the Palestinians.\textsuperscript{48} It was stressed, however, that the weapons to be supplied were purely defensive, and that they would be supplied with Israel’s consent and via Israeli territory. In 2010 Russia officially transferred 50 BTR-70 APCs to the Palestinian National Administration free of charge. The hardware was left in storage in Jordan pending Israeli permission to make the actual delivery.\textsuperscript{49}

To summarize, Russia maintains and develops friendly relations with the Palestinian Autonomy—but in a delicate manner, trying to work within the rules that have come to exist in this complex part of the world.

\textbf{THE SHIA STATES: DEALS UNDER U.S. PRESSURE}

\textbf{IRAQ}

Since the 2003 change of government in Baghdad, Russian defense exports to Iraq have been limited to only a few Mi-17 multirole helicopters. The bulk of the Iraqi defense market is now controlled by the United States, which accounts for about 85 percent of Iraqi weapons imports.\textsuperscript{50} There was, however, a major new development in mid-2012, when Russia and Iraq agreed a package of weapons contracts worth 4.2 billion dollars. These included orders for 48 Pantsir-S1 gun-missile air defense systems (2.2 billion dollars); 36 Mi-28NE attack helicopters (2 billion dollars); and other weaponry. There were also reports claiming that Baghdad might soon place an order for MiG-29M/M2 fighters.\textsuperscript{51} The signing of one of the largest contracts between Russia and Iraq in recent history was taken as an indication that the Shia-led government in Baghdad was trying to pursue a more independent foreign policy and end its utter dependence on Washington. But, shortly after the deal was signed, various parties—including some Iraqi officials—began to question it, and to insist that the agreements with Russia must be reviewed over allegations of corruption. It still remains unclear whether, when, and to what extent the contracts will be fulfilled. Meanwhile, Washington continues to put a great deal of pressure on Baghdad over this issue because it does not want Russia to strengthen its position in the region.

If, however, all the Russian–Iraqi arms contracts are fulfilled despite U.S. pressure, Russia will become the second-largest supplier of weapons to Iraq after the United States. The value of its arms exports to Iraq will be about 30 percent of the projected U.S. figure (which stands at 12.3 billion dollars\textsuperscript{52}). Meanwhile, Ukraine has also been strengthening its cooperation
with Iraq, and could well claim third position in the ranking of top arms exporters to the
country, with potentially more than 2 billion dollars’ worth of sales.

IRAN

In view of its international isolation, Iran is aiming for self-sufficiency in defense matters.
Cooperation between Iran and Russia was fairly active during the implementation of the
package of agreements signed in 1989–1991. As part of those agreements, Iran received
MiG-29 and Su-24MK aircraft, S-200VE SAM systems, and three Project 877EKM subma-
rines. The agreements included local production in Iran of Russian T-72S tanks and BMP-2
infantry fighting vehicles.

Russia ended that cooperation in the late 1990s after coming under pressure from the
Americans.

After 2000 Russian–Iranian military and technical cooperation was resumed, but it remained
fairly limited. The largest contracts signed since then have been for Tor-M1 SAM systems,
Su-25 ground attack aircraft, and Mi-17 helicopters. Negotiations and contacts continued,
on and off, in the subsequent years; they were complicated by the exceptional political
situation over the Iranian nuclear program and the international reaction to that program.

Whenever Russian companies resumed arms supplies to Iran, they would always come under
U.S. sanctions. The list of these companies includes Russian makers of aircraft, missiles, and
air defense systems, such as the Instruments Design Bureau (KBP), Sukhoi, and the state
intermediary Rosoboronexport.

Tensions subsided briefly once again in 2007, when Tehran hosted a meeting of the Russian–
Iranian intergovernmental commission for military and technical cooperation. After the meeting
Russia announced its intention to continue such cooperation with Iran. But in the spring of
2010 it became clear that Iran was going to come under even tougher UN Security Council
sanctions, which Russia would have to (and eventually did) support, for a variety of reasons.

UN Security Council Resolution 1929 was passed on June 9, 2010. On September 22, 2010
the Russian president issued a decree ordering measures to comply with the resolution. Those
measures included a ban on any transfers to Iran of main battle tanks, armored
combat vehicles, combat aircraft, attack helicopters, military ships, missiles and missile
systems, the S-300 SAM systems, or any related hardware, including spare parts.

During the brief détente, Russia and Iran were in negotiations over a whole package of
contracts. These included an order for 50 RD-33 aircraft engines, which Iran wanted for its
Azarakhsh supersonic fighter-bombers; the development of a modified version of the Ka-32
helicopter especially for Iran, and mass production of these helicopters in Iran; and the repair
of Iran’s Project 877EKM submarines. Moscow and Tehran also discussed a contract for Su-
30 and MiG-29SMT fighters; Iskander-E theater ballistic missiles; T-90S tanks; Nona-K
towed artillery systems; and other hardware. The Iranian Navy expressed interest in Russian-
made missile, amphibious landing, and patrol boats, as well as corvettes. Both sides also
spoke about other potential areas of military and technical cooperation, including the
development of space communication and Earth imaging systems, and production of ground
and naval weaponry in Iran under Russian license. In addition to these talks, in 2007 Russia
made actual deliveries of 29 Tor-M1 SAM systems, including 1,200 missiles.

The most important event during that period was the signing of a contract for five batteries of
the S-300PMU-1 SAM systems, worth an estimated 800 million dollars. But after Russia
supported the arms embargo on Iran in June 2010, it refused to go ahead with the deal.

Iran reacted angrily, accusing Russia of being an unreliable partner, and announced that it
was developing indigenous SAM systems with a similar capability. It is clear that even if the
sanctions are lifted at some point in the future, Iran is unlikely to buy weapons from Russia; it
will probably prefer to take its custom to China (in fact, it is already doing just that) and
other, more agreeable suppliers. Iran has also filed a 4 billion-dollar claim against Russia at a
court of arbitration in Geneva; proceedings have been under way since the spring of 2011.
Russia has returned only the Iranian deposit of 166.8 million dollars under the failed contract;
it has also been trying to get Iran to drop its legal action, but without any results so far.
Russian losses resulting from its decision to suspend military and technical cooperation with Iran are estimated at 11–13 billion dollars; the figure includes not only the contracts that have fallen through, but lost opportunity as well. Russian–Iranian defense cooperation continues in only a small number of areas that do not fall under the scope of the UN Security Council resolution. According to some odd bits of information, these areas may include upgrading previously supplied Su-24MK aircraft and repairing Iranian submarines. Russian defense exports to Iran are expected to reach a mere 60 million dollars by 2015, down sharply from 1.68 billion dollars in 2004–2007, and 410 million dollars in 2008–2011.

Given the difficult political situation in the Middle East in general, and the crisis over the Iranian nuclear program in particular, Russia is unlikely to sign any large new weapons contracts with Iran over the next few years. It is safe to say that military and technical cooperation between the two countries has been completely suspended, and will not be resumed any time soon.

TURKEY: CAREFUL BARGAINING

Turkey has been making great progress over the past decade. That progress has enabled the country to ramp up its military capability and become a regional power potentially capable of playing a dominant role in resolving military-political problems in southern Europe and the eastern Mediterranean. So far, however, Turkey has been unable to normalize its relations with Greece, or to sort out its problem with the Kurds.

Turkey’s military spending has been growing steadily; it topped 18 billion dollars in 2012. The Turkish armed forces are the second most numerous among the NATO countries. The Turkish defense market is worth an estimated 3–5 billion dollars; it has traditionally been dominated by such arms suppliers as the United States, Britain, France, and Germany. China, Bulgaria, Romania, and Ukraine have also secured some sales in recent years.

Turkey bought 12.813 billion dollars’ worth of weapons in 2004–2011; by that indicator it ranks fourth in the Middle East after Saudi Arabia, the UAE, and Egypt. By 2015 the country is expected to buy another 11.36 billion dollars’ worth of weapons.

Russian–Turkish military and technical cooperation has a long history. In terms of recent decades, it resumed in 1992. The Turkish border service and gendarmerie brigades have received Russian BTR-60 and BTR-80 APCs, Mi-8MTSh/Mi-17 multirole helicopters, Kalashnikov assault rifles and machine guns, Dragunov sniper rifles, RPG-7 hand-held anti-tank grenade launchers, MLR systems, and other weapons.

In 1994 Russia and Turkey signed an intergovernmental agreement on military-and-technical and defense industry cooperation. In May 2001 the two governments set up a joint Russian–Turkish commission on military and technical cooperation. In December 2004 they also signed an agreement on mutual protection of intellectual property in the area of military and technical cooperation, and another agreement on mutual protection of secret information in the same area.

Although Russia and Turkey have put in place an extensive legal framework for military and technical cooperation, the prospects for such cooperation are limited, for a variety of obvious reasons. One of them is that Turkey uses NATO weapons standards. Another is that Russian suppliers face stiff competition in the Turkish market from the United States and other Western countries, which have a lot of influence on Turkey’s military and political establishment. Some time ago Russia proposed to begin production under Russian license in Turkey of T-80/T-90 tanks adapted to NATO ammunition standards, as well as BTR-80/BTR-90 APCs and Tigr armored vehicles. Russia was also willing to supply short- and medium-range anti-tank missile systems; jointly build search and rescue ships; integrate the Strelets SAM system with a similar Turkish system called Aselsan; and pursue joint military space projects. None of these proposals has been implemented, and the situation is unlikely to change any time soon.

Russian arms exports to Turkey have been very limited over the past few years. Russia has supplied 80 Kornet-E anti-tank missile systems worth 70 million dollars, and signed a 5 million-dollar contract to repair five Mi-17TV-1 multirole helicopters previously supplied to
The Middle East faces an era of fundamental change. The Middle East, long defined by the region’s geopolitical fault lines and intricate power dynamics, is undergoing a profound shift. The end of the Cold War and the rise of new actors, including Iran, continue to redefine the region’s landscape. The Middle East is no longer a bipolar world with clear-cut alliances and defined interests. Instead, it is a complex web of overlapping interests and competing ambitions.

In recent years, cooperation between Turkey and the two former Soviet republics has been growing steadily. The Turkish government, under President Recep Tayyip Erdogan, has taken a more assertive role in the region, seeking to strengthen its influence and secure its strategic interests. This shift has led to new dynamics in the Middle East, with Turkey playing a more prominent role in regional affairs.

The Middle East is also witnessing a significant increase in economic and cultural exchanges. The region’s economies are becoming more integrated, with trade flows increasing and cross-border investments growing. This is particularly true in the energy sector, where the region’s oil and gas reserves are attracting significant investment from international companies.

However, despite these developments, the Middle East remains a region of significant challenges. Political instability, terrorism, and the ongoing conflict in Syria continue to cast a shadow over the region. Despite these difficulties, there are signs of hope and cooperation, with initiatives being taken to address these challenges and promote regional peace and stability.

In conclusion, the Middle East is undergoing a period of significant change. While there are challenges, there is also potential for cooperation and growth. The region’s leaders must work together to navigate this new landscape and ensure a brighter future for its peoples.
The continuing arms race in the Middle East, coupled with the region’s Islamization, may pose serious challenges to Russia, especially near its southern borders. On the whole, a destabilization in the South Caucasus is making the threats to Russian security originating in the Middle East even more pressing. In view of these threats, Russia must take more energetic action—including a revision of its Middle East arms exports policy—in order to prevent possible use of military force in the region.

One of the measures that could reduce the potential for conflict in the Middle East would be for all the exporter countries to introduce a moratorium on arms supplies to the region. If Russia were to propose such an initiative, it would significantly augment its international standing and reputation.

NOTES


2 Iran’s share as a destination of Russian arms exports peaked at 16.2 percent in 2006. The figure stood at 4.2 percent in 2004; 0.8 percent in 2005; 16.2 percent in 2006; 9.4 percent in 2007; 0.8 percent in 2008; 3.2 percent in 2009; 2.3 percent in 2010, and 0.1 percent in 2011.

3 There were no identified deliveries in 2004–2006. In 2007 the figure stood at 1.5 percent; it peaked at 8.9 percent in 2008, then fell to 5 percent in 2009; 4.5 percent in 2010; and 3 percent in 2011.

4 There were no identified deliveries in 2004–2005. In 2006 the figure stood at 5.1 percent; it peaked at 8.2 percent in 2007, then fell to 2.3 percent in 2008; 1.5 percent in 2009; 1.3 percent in 2010; and 3.7 percent in 2011.

5 There were no identified deliveries in 2004–2007. The figure stood at 0.8 percent in 2008 and 2.6 percent in 2009; it peaked at 4.9 percent in 2010; then fell to 3.4 percent in 2011.


4. https://www.autosportsnews.com/2012/01/25/2012-worlds-most-competitive-market-fourth-quarter/201212051210".


35 The contract for 36 Yak-130UBS combat trainers was signed in late 2011; the value of the deal is 550 million dollars, but it is unlikely to be fulfilled within the original time frame due to the ongoing crisis. For more details, see: “Syria Buys Yak-130 Combat Trainers,” Oruzhiye Rossii, January 23, 2012, <http://www.armsexpo.ru/049051124050054053051049.html>, last accessed August 6, 2014.

36 It is known, for example, that in 2012 Russia completed repairs and upgrades of 20 Syrian Mi-25 attack helicopters, but it delayed the return of these helicopters to Damascus due to the ongoing civil war. For details, see: “Delivery Deadline for Syrian Mi-25 Helicopters Pushed Back,” Oruzhiye Rossii, July 21, 2012, <http://www.armsexpo.ru/0490511240500560555505.html>, last accessed August 6, 2014.

37 For example, in October 2012 Turkey forced a civilian flight from Moscow to Damascus with 35 passengers on board to land at a Turkish airport because Russian military cargo was carried. The cargo was confiscated by Turkey (12 containers with military equipment from the Tula-based Instruments Design Bureau; more specifically, the cargo was carrying radio-technical components that fall under the definition of dual-use technology). Russia argued that supplying dual-use technology was not prohibited by any international conventions. For details, see: “Turkey Forces an Armenian Plane to Land at a Turkish Airport,” Vzglyad, October 15, 2012, <http://vz.ru/news/2012/10/15/602585.html>, last accessed August 6, 2014.


39 Attempts to restrict military and technical cooperation between Russia and Syria were also made before: it was claimed that the weapons supplied to Syria end up in the hands of terrorist organizations, including Hezbollah, or are illegally re-exported to Iran. The sale of P-800 Yakhont supersonic cruise missiles, which are part of the Bastion coastal defense system, drew especially sharp criticism from the United States and Israel. It appears that Russia has not officially relinquished that contract.

40 Russia has not officially refused to fulfill the contracts for air defense systems signed previously with Syria. In late May 2013 there were even reports that Russia had delivered S-300 SAM systems to Syria; but in actual fact Russia had supplied only the individual components; exports of the complete SAM systems to Syria have been halted. See: “S-300 will not save Syria,” Vedomosti, September 5, 2013, No. 162 (3432), <http://www.vedomosti.ru/politics/news/15986151/s-300-siriyu-ne-spasut>, last accessed August 6, 2014.


42 RPG-32 Hashim is a multi-caliber handheld grenade launcher named in honor of Prophet Muhammad’s great-grandfather Hashim Abd Ad-Dar, from whom the Jordanian royal family traces its lineage.


63 The companies bidding for the Turkish contract include Raytheon and Lockheed Martin with the PAC-3 Patriot system; Rosoboronexport with the S-300; China’s CPMIEC with the HQ-9 (a modified copy of the Russian S-300V system); and Europe’s Eurosam consortium with the SAMP/T Aster 30.

64 This value of this shortfall equals almost half of Russia’s current portfolio of defense contracts, which is worth 46 billion dollars.

65 Military and technical cooperation with the North African countries is not analyzed in any great detail in this review; nevertheless, the overall military-political situation in some of these countries is just as complex as in the Middle East. It is worth noting that of the entire North African region, Russia has suffered the largest arms trade losses in Libya (about 4 billion dollars).
Olga Skorokhodova

MYANMAR MANIA AND THE LESSONS FOR RUSSIA*

The political landscape of the Republic of the Union of Myanmar, previously known as Burma (the CIA World Factbook continues to use the old name),¹ has undergone serious changes in the past several years. While the rest of the world was seeking ways out of yet another economic crisis, Myanmar managed not only to recover from the devastating consequences of Cyclone Nargis, which had claimed over 138,000 lives, but also to adopt a new constitution based on the principle of discipline-flourishing democracy, as well as holding nationwide parliamentary elections. A new political period thus began in the history of Myanmar.

The new head of state, President Thein Sein, released the pro-democracy campaigner and Nobel Laureate Aung San Suu Kyi after nearly 15 years of house arrest, permitting her to engage in political activity. The abolition of censorship and of the state monopoly on the media resulted in a sharp growth in the number of newspapers and other news outlets. The international community, particularly the classical liberal democracies was excited to observe these changes in the country which until recently has been described as an outpost of tyranny, alongside Somalia, Belarus, North Korea, and Iran. Patrick Cronin, senior advisor and senior director of the Asia-Pacific Security Program at the Center for a New American Security, coined the term Myanmar mania² to describe this excitement, that one could compare with the Gorbymania of the 1980s.

ASIA’S KLONDIKE? THE SPECIFICS OF DOING BUSINESS IN MYANMAR

One aspect of Myanmar mania is the investment rush that has seized the international business community. The explanation is simple: one of the largest Southeast Asian countries in terms of territory, Myanmar possesses a wealth of natural resources. There are oil and gas, precious stones and metals, etc. The world probably does not even come close to appreciating the true scale of Myanmar’s natural wealth: there have never been any attempts to prospect for many of the potential valuable minerals there. Myanmar’s subsoil resources remain untapped, forming the foundation for a strong economic future. Given that the country’s demographic potential is as sizeable as its natural wealth, the McKinsey consultancy’s prediction that the Myanmar GDP will grow fourfold by 2030 does not appear to be far off.³

Thein Sein’s reformist approach both earned him a fairly good personal reputation within democratic circles and opened up a floodgate of foreign investment into the Myanmar economy, which had previously been impossible owing to Western sanctions against the country’s military junta. (We are speaking here about the U.S. and EU sanctions; Washington’s proposal to impose UN-wide sanctions against Myanmar was blocked by Russia and China in 2007).

Building a disciplined democracy requires not just finances but also—and more importantly—new technologies. According to the IMF, foreign direct investment in Myanmar doubled between 2008 and 2012 to reach $1.4 billion (see Figure 1), yet there is still room for growth. Laos, whose population is only 10 percent of the Myanmar figure, received the same amount of investment in 2012 alone.⁴
Even though foreign presence in the Myanmar economy has grown in size and scale, the IMF report states, "the Myanmar economy should be measured and graded on the basis of the results, which will immediately become evident to foreign investors." That said, the opening of the country to foreign investment is not the easiest country for doing business. The World Bank's Doing Business report ranks Myanmar as the 189th easiest country for doing business. The World Bank's Doing Business report ranks Myanmar as the 189th easiest country for doing business.

"Even though foreign presence in the Myanmar economy has grown in size and scale, the IMF report states, "the Myanmar economy should be measured and graded on the basis of the results, which will immediately become evident to foreign investors." That said, the opening of the country to foreign investment is not the easiest country for doing business. The World Bank's Doing Business report ranks Myanmar as the 189th easiest country for doing business. The World Bank's Doing Business report ranks Myanmar as the 189th easiest country for doing business.

"Even though foreign presence in the Myanmar economy has grown in size and scale, the IMF report states, "the Myanmar economy should be measured and graded on the basis of the results, which will immediately become evident to foreign investors." That said, the opening of the country to foreign investment is not the easiest country for doing business. The World Bank's Doing Business report ranks Myanmar as the 189th easiest country for doing business. The World Bank's Doing Business report ranks Myanmar as the 189th easiest country for doing business.

"Even though foreign presence in the Myanmar economy has grown in size and scale, the IMF report states, "the Myanmar economy should be measured and graded on the basis of the results, which will immediately become evident to foreign investors." That said, the opening of the country to foreign investment is not the easiest country for doing business. The World Bank's Doing Business report ranks Myanmar as the 189th easiest country for doing business. The World Bank's Doing Business report ranks Myanmar as the 189th easiest country for doing business.

"Even though foreign presence in the Myanmar economy has grown in size and scale, the IMF report states, "the Myanmar economy should be measured and graded on the basis of the results, which will immediately become evident to foreign investors." That said, the opening of the country to foreign investment is not the easiest country for doing business. The World Bank's Doing Business report ranks Myanmar as the 189th easiest country for doing business. The World Bank's Doing Business report ranks Myanmar as the 189th easiest country for doing business.

"Even though foreign presence in the Myanmar economy has grown in size and scale, the IMF report states, "the Myanmar economy should be measured and graded on the basis of the results, which will immediately become evident to foreign investors." That said, the opening of the country to foreign investment is not the easiest country for doing business. The World Bank's Doing Business report ranks Myanmar as the 189th easiest country for doing business. The World Bank's Doing Business report ranks Myanmar as the 189th easiest country for doing business.

"Even though foreign presence in the Myanmar economy has grown in size and scale, the IMF report states, "the Myanmar economy should be measured and graded on the basis of the results, which will immediately become evident to foreign investors." That said, the opening of the country to foreign investment is not the easiest country for doing business. The World Bank's Doing Business report ranks Myanmar as the 189th easiest country for doing business. The World Bank's Doing Business report ranks Myanmar as the 189th easiest country for doing business.

"Even though foreign presence in the Myanmar economy has grown in size and scale, the IMF report states, "the Myanmar economy should be measured and graded on the basis of the results, which will immediately become evident to foreign investors." That said, the opening of the country to foreign investment is not the easiest country for doing business. The World Bank's Doing Business report ranks Myanmar as the 189th easiest country for doing business. The World Bank's Doing Business report ranks Myanmar as the 189th easiest country for doing business.

"Even though foreign presence in the Myanmar economy has grown in size and scale, the IMF report states, "the Myanmar economy should be measured and graded on the basis of the results, which will immediately become evident to foreign investors." That said, the opening of the country to foreign investment is not the easiest country for doing business. The World Bank's Doing Business report ranks Myanmar as the 189th easiest country for doing business. The World Bank's Doing Business report ranks Myanmar as the 189th easiest country for doing business.

"Even though foreign presence in the Myanmar economy has grown in size and scale, the IMF report states, "the Myanmar economy should be measured and graded on the basis of the results, which will immediately become evident to foreign investors." That said, the opening of the country to foreign investment is not the easiest country for doing business. The World Bank's Doing Business report ranks Myanmar as the 189th easiest country for doing business. The World Bank's Doing Business report ranks Myanmar as the 189th easiest country for doing business.
There are political and economic reasons for this low rating. Political risks include possible destabilization of the political situation in the country and the continuing uncertainty as to Myanmar’s future after the 2015 general election.

We will dwell in detail on the economic factors hampering the development of foreign business in Myanmar. These factors could be further subdivided into financial and bureaucratic/institutional.

To begin with, it turns out that doing business in Myanmar is rather costly. The inelastic and unsaturated Myanmar market responded to the beginning of the investment boom in a very predictable manner. Hotel rates in Yangon are reported to have grown between twofold and threefold. Renting a square meter of office space in Yangon, which retained the status of Myanmar’s business capital after the political capital moved to Naypyidaw, now costs $100 per month, compared with $74 in Singapore. Housing rents have skyrocketed, reaching $6,500 for a standard three-room apartment. The recent spate of terrorist attacks has forced landlords to invest more in security by installing CCTV cameras, metal detectors and other equipment. All this is driving accommodation prices up further.

The country’s fiscal policy also leaves much to be desired. The overall tax burden stands at 48.9 percent. The consultancy KPMG recommends that anyone looking to launch a business in Myanmar start by setting up a holding company in a neighboring country. In Singapore, for example, the corporate tax rate is 17 percent, against 25 percent in Myanmar, while the capital gains tax under a bilateral agreement is 10 percent (40 percent in Myanmar).

As for the bureaucratic and institutional barriers, it should be noted that the paperwork involved in the opening of a business in Myanmar may take up to 72 days to complete, with the applicant having to engage in 11 different registration procedures. In addition, Myanmar’s legislation requires the applicant to hold at least $58,000 in their account before launching a business. Compare this with the 10,000 roubles ($270) required in Russia.

Additionally, Myanmar is not the highest-achieving country in terms of contract performance: it holds the penultimate 188th position in the global ranking in this category. Settling a contractual conflict may take up to three years and 55 percent of the contract’s value.

Like many other Third World countries, Myanmar suffers from an extremely non-transparent government system: Transparency International ranks it 172nd out of 176 countries for perceived corruption (the lower the number, the higher the corruption level). Only Sudan, Afghanistan, North Korea, and Somalia are even worse for corruption, according to the report.

One huge obstacle to attracting new investors is the current absence of a stock exchange in Myanmar. The opening was originally set for 2015, but this deadline now appears to be slipping because the country lacks both qualified personnel to run the future exchange and companies that could trade there. At present, there are only five Initial Public Offering (IPO)-capable Myanmar firms, whereas at least 80 are required to qualify for the opening of a stock exchange. The only solution is to allow foreign companies to IPO in Myanmar. It is for this purpose that the Myanmar government is planning to revise the Myanmar Companies Act, which was passed in 1914 and still remains in force.

Apart from the stock market problems, the country’s finance, security, and bond markets are still in their infancy. Experts acknowledge that liberalizing the financial market and opening it to foreign capital is sine qua non.

On the other hand, the situation with cash machines and payment terminals is rapidly improving. Three international payment systems came to Myanmar in the last quarter of 2012 and throughout 2013: MasterCard, Visa, and American Express. MasterCard authorized seven local banks to issue MasterCard banking cards; these banks installed 285 payment terminals in Yangon and 210 cash machines across the country (including 130 in Yangon). Visa licensed eight banks, which own 550 payment terminals and 200 ATMs between them. The Chinese bank UnionPay, which has branches across the globe, set up a local operation called Myanmar UnionPay, which comprises 17 offices and 1,655 payment terminals. The luxury of paying with a credit card is gradually becoming affordable not just to tourists and expatriates but also to local residents. On October 8, 2013, MasterCard and Myanmar’s Cooperative Bank (CB Bank) unveiled the country’s first debit card for local customers.
The Russian company will have a 30 percent stake in the project.

Investment under a production sharing agreement, as mandated by the new foreign investment holding under a production sharing agreement, will work in conjunction with the Myanmar Rm, which opened a branch in 2013. It was a joint venture with the country in 2012. The government of Myanmar, under the Minister of Energy, unfortunately, the same as its predecessor’s, the Chinese company has been seeking approval for a project in 2012.

Russia’s flag is the only one to appear in this article.

In the Myanmar market, there are no real rebranding services. The coming of Myanmar’s securities market, which is a recent development, has not been able to offer the sort of services that the Russian company has.

A draft law on banking operations was expected to be made public by the end of 2014. Also, in the Myanmar market, there are no real rebranding services. The coming of Myanmar’s securities market, which is a recent development, has not been able to offer the sort of services that the Russian company has.

Gary K. Wynn, Morgan Stanley's chief executive, is taking part in the extraction of natural gas, which is the country’s main export, copper, molybdenum, and zinc.

There are also stakeholdings in metal mining, the Russian company. In 2012, the Russian company built a new metal mining facility in Yunnan.
Victorious Glory International (VGI) jointly with a local partner began developing a rare-earth metals deposit in 2007 but then ran into serious difficulties.

It should be noted that the spectrum of current Russian investments in Myanmar is fairly traditional: Russian business mostly invests in the mining, primary, energy, and metallurgy sectors, and Myanmar is no exception here.

So far Russian business has made rather modest progress in Myanmar, despite the fact that the two countries’ trade and economic relations used to be quite active several years ago, especially in the area of arms trade. Russia sold Mil Mi-35 helicopters and MiG-29 fighter jets to Myanmar in the 2000s, as well as artillery and air defense systems. It is assumed that Russian investors should find it easier to enter the Myanmar market as compared with their rivals hailing from those countries that supported the sanctions against Yangon.

Education is another area of active Russian–Myanmar contacts. Thanks to the efforts of Russian Ambassador to Myanmar Gleb Ivashentsov, Myanmar students have studied at Russia’s leading educational establishments since 1997, mostly at Myanmar’s expense. According to previously unreported statistics obtained from the Russian Education and Science Ministry, a total of 4,705 Myanmar students have completed courses of studies in Russia in the past 20 years. There were 825 students in the 2013/2014 academic year; only one of them was studying at the expense of the Russian budget.

A detailed analysis of these figures yields a very interesting breakdown in terms of the areas of study (see Table 1). It appears that Russian universities have brought up Myanmar’s technical elite in less than 20 years. Unfortunately, in the light of the investment race currently observed in Myanmar, Russian business has been failing to appreciate and avail of this competitive advantage. It is important to understand that Myanmar does not cooperate in education on such a grand scale with any other country, perhaps with the only exception of China, and that Russia cannot boast such extensive education ties with many other ASEAN nations.

The Myanmar graduates of Russian universities represent the pro-Russian segment of the Myanmar elite; they contribute to the forming of favorable attitudes towards Russia in the Myanmar political arena. Upon obtaining their master’s or even doctoral degrees in Russia, they return to Myanmar to take up leadership posts. Furthermore, they possess knowledge of Russian production technologies.

This factor is of most pragmatic importance in a country like Myanmar, where foreign investments are impossible without giving employment to the local workforce. Under the new foreign investment law, by the end of the first five years of operation the share of Myanmar personnel in a joint venture should stand at not lower than 25 percent, after 10 years at 50 percent; after 15 years at 75 percent. It is the employer’s obligation to organize on-the-job training for the local workforce. The investor is obliged to hire only local residents

<table>
<thead>
<tr>
<th>Area of study</th>
<th>Students</th>
</tr>
</thead>
<tbody>
<tr>
<td>Medicine</td>
<td>138</td>
</tr>
<tr>
<td>Construction</td>
<td>38</td>
</tr>
<tr>
<td>Mechanical engineering and instrumentation</td>
<td>517</td>
</tr>
<tr>
<td>Metallurgy</td>
<td>13</td>
</tr>
<tr>
<td>Aeronautical engineering</td>
<td>260</td>
</tr>
<tr>
<td>Applied mathematics and information sciences</td>
<td>1,870</td>
</tr>
<tr>
<td>Physics</td>
<td>119</td>
</tr>
<tr>
<td>Power engineering, including nuclear power engineering</td>
<td>256</td>
</tr>
<tr>
<td>Mining engineering</td>
<td>66</td>
</tr>
<tr>
<td>Chemistry and materials science</td>
<td>492</td>
</tr>
</tbody>
</table>

**Total students over 20 years** 4,705

Tuition-paying Myanmar students in Russia in 2013 828

**Total Myanmar students in Russia in 2013** 829
Russia’s Foreign Policy and Its Economic Presence in Myanmar

Russia’s foreign policy towards Myanmar is characterized by a strategic approach aimed at expanding its economic footprint and strategic influence in the region. Despite the regional landscape being dominated by China and other major powers, Russia seeks to establish a strong presence in Myanmar through various bilateral and multilateral initiatives. This is evident in the country’s investments, trade agreements, and diplomatic engagements.

Despite geopolitical complexities and historical challenges, Russia has been active in Myanmar, particularly following the 2010 military coup and the subsequent democratic reforms. The country’s strategic location, extensive coastline, and rich natural resources present significant opportunities for Russia to strengthen its economic ties and regional influence.

Economic Interactions:
- **Trade**: Russia and Myanmar have potential for increased trade in commodities such as timber, rice, and oil. The two countries have signed several agreements to enhance bilateral trade, with an eye on diversifying Russia’s economic portfolio.
- **Investment**: Russian investors have expressed interest in Myanmar’s infrastructure development, energy sector, and agriculture. Notable projects include the construction of a hydroelectric power station.
- **Agriculture**: Russia has invested in Myanmar’s agricultural sector, focusing on the development of commercial farms and agro-industries.

Despite geopolitical uncertainties, Russia’s determined efforts to establish a strong economic presence in Myanmar reflect a strategic calculus aimed at balancing regional powers and securing its strategic interests in Southeast Asia.

**Understanding the Russian Perspective**

Russia’s engagement in Myanmar is part of a broader strategy to influence the geopolitical dynamics in the region. By establishing a strong economic presence, Russia seeks to influence policy decisions and enhance its strategic leverage in the broader context of China’s Belt and Road Initiative (BRI) and other regional cooperation frameworks.

**Strategic Significance for Russia**

- **Political Alliances**: Russia’s presence in Myanmar can help it align with regional powers and maintain a balance of power in Southeast Asia.
- **Economic Interests**: Russia’s economic interests in Myanmar are tied to its desire to diversify its energy sources and establish a footprint in a region rich in natural resources.
- **Military Cooperation**: Russia may seek to enhance military cooperation with Myanmar, offering advanced military equipment and training, as part of a broader strategy to counterbalance China’s military presence in the region.

In conclusion, Russia’s foreign policy towards Myanmar is a testament to its strategic vision in the broader context of regional dynamics. By fostering economic and political linkages, Russia aims to ensure its influence remains a significant factor in the region's evolving geopolitical landscape.
meeting of the newly established commission; the list includes Bashneft, Inter RAO, Sukhoi Company, and the United Aircraft Corporation. However, while a convenient interface for bilateral economic cooperation has been provided, its further perspective and dynamics largely depend on what particular cooperation proposals and initiatives both from Russia and from its East-Asian counterpart would fill it.

SEARCHING FOR NON-TRIVIAL SOLUTIONS: WHAT COULD RUSSIA AND MYANMAR OFFER EACH OTHER?

A Deutsche Bank Markets Research report entitled Russia’s Outward FDI: in Search of New Paradigm mentions, among others, three variables that influence the foreign investment choices of Russian business: the size of the country’s economy, the presence of natural resources, and the share of the service industry. For example, a country’s GDP growth of 1 percent correlates with a 0.4 percent growth in Russian investments in that country. If the share of the natural resources exports grows by 1 percent, Russian investments in that country grow by 0.5 percent.

This model indicates that Asia will turn into a major destination for Russian foreign investment in the near future. Myanmar looks particularly appealing in this sense: with its projected economic growth at 7–8 percent in the next few years and mostly untapped resources, the country has been described as the last frontier in both Asia and the world.

Myanmar and Russia, therefore, have all the requisite ingredients and even a number of competitive advantages for large-scale cooperation in investments and trade. The wait-and-see attitude effected by Russian business several years ago as applied to the battle for Myanmar was fairly justified up to a point: the absence of even rudimentary banking instruments, financial institutions, or insurance mechanisms made doing business in that country too risky. Russia’s capitalism is only 20 years old, and the country’s companies lack the safety net available to businesses in the United States and Western Europe. However, the Myanmar government is doing a lot to make the life of foreign companies easier, and these efforts are starting to pay off. The expert community is unanimous in the opinion that the time has come for the Russian business to become more active in Myanmar in order to avoid paying high a high entry cost several years later.

One should not overrate the political risks of doing business in Myanmar. After all, Russian investors are quite used to volatile conditions and should have grown immune to them by now. Risks are a systemic component of any developing market, and the risks in Myanmar are not at all high compared with those in the Middle East, for example. What is needed is an understanding of what is holding back the transformation of the favorable conditions and competitive advantages into specific Russian–Myanmar projects, and also an idea of which sectors of Myanmar’s economy would be the most cost-effective to Russian companies.

One of the primary factors underlying the modest size of Russian–Myanmar economic cooperation to date is the absence of bilateral agreements and institutions that would support it. Myanmar and Russia have yet to sign a framework treaty for trade and economic cooperation, although the first step in this direction was taken in August 2014 with the establishment of the Intergovernmental commission.

Even though a trade treaty is not a panacea, it could additionally stimulate contacts between the two countries’ private and public sectors. The creation of an intergovernmental commission, for its part, could pave the way for the signing of industry-specific agreements.

The fact that Russia does not have a trade mission in Myanmar (the Soviet Union used to have one) indicates the institutional and contractual lassiness of bilateral relations. A recent report by the Russian Ministry of Economic Development says that the need for Russian trade missions in a number of countries, including Myanmar, has been actively discussed of late. This suggests that the topic has not even been put on the Russian government’s agenda yet. The Russian Chamber of Commerce and Industry has no immediate plans to open a representative office in Yangon, either, because doing so would require funding from companies interested in having such an office. In the meantime, the American Chamber of
The Russian economy is now the world's second largest after China. Russia, however, is also the world's largest oil producer and second largest gas producer. The country's economy is heavily dependent on energy exports, which account for about 40% of total exports. Russia is also a major exporter of high-tech products and services, including software and IT services. However, the country's economy is vulnerable to fluctuations in global oil prices, which have a significant impact on the country's revenue and foreign exchange reserves.

The Russian government has been implementing a series of economic reforms aimed at modernizing the economy and improving its competitiveness. These reforms include structural reforms to the energy sector, the introduction of a single digital economy, and the promotion of innovation and entrepreneurship. The government has also been focusing on improving the business environment and reducing corruption, which has been a major obstacle to economic growth.

Despite these efforts, the Russian economy remains vulnerable to external shocks, particularly in the energy sector. The country's economic growth has been slow, and the unemployment rate remains high. The government has been implementing fiscal and monetary policies to support the economy, including increasing government spending and providing support to businesses.

The Russian economy is also facing challenges related to demographic trends, including an aging population and declining workforce. The government has been implementing policies to address these challenges, including increasing the retirement age and promoting the birth rate.

Overall, the Russian economy is undergoing significant changes, with a focus on modernization and reform. The government is committed to implementing these changes, and the economy is expected to continue to grow in the coming years.
commodities. We should note that the EU in 2013 included Myanmar in its generalized scheme of preferences.

Equally important is greater use of the opportunities offered by alliances with Myanmar companies: both with local businesses, as already demonstrated by Bashneft and Nobel Oil, and with veteran players on the Myanmar market, including Chinese ones. This tactic would help achieve several objectives at once by reducing the number of potential rivals, mitigating potential economic risks, and pre-empting China’s possible negative reaction to Russia’s advance to the markets which Beijing believes to be within its sphere of interests in the same manner as Russia believes it has special rights to the former Soviet republics.

Finally, it is important to identify those Myanmar industries in which Russian business could participate, given its general and region-specific foreign investment experience. Myanmar’s development needs should be appraised alongside the opportunities provided by the country’s existing human potential.

We may predict with considerable confidence that Russia’s advance into the Myanmar market will be led by major companies. This traditional tactic is fairly justified at this stage, because Myanmar needs to implement massive long money projects with protracted payback periods.

First of all, it is fairly possible that the Russian oil-and-gas giants Gazprom and Rosneft, which need to expand their resource base and adapt their strategies to the Western sanctions, would enter the Myanmar market.

There is also massive demand for electricity in Myanmar: according to various estimates, only 30 percent of the population has access to the power grid. Power blackouts or total absence of electricity supply hamper the development of other industries, from tourism to metallurgy. Myanmar’s combined generation capacity stands at about 3,500 MW. Ironically, according to UN data, Myanmar is the world’s 13th country for water resources. Yet it uses no more than 1 percent of those resources for power generation, even though its generation potential is estimated at 100,000 MW.57

Myanmar’s huge demand for electricity is matched by its equally gigantic generation potential. The Russian corporation RusHydro has plenty of experience in developing power-generation projects in Asia Pacific, including in Vietnam. However, as we were told by company sources, RusHydro has no immediate plans to launch a project in Myanmar. One possible explanation is the company’s financing difficulties. This, however, does not affect the potential benefits of Russian–Myanmar cooperation in the power-generation sector. It should be noted that 256 Myanmar students have obtained degrees in power generation from Russian universities.

Myanmar offers equally broad opportunities to the Russian nuclear specialist Rosatom, which signed an intergovernmental cooperation agreement with the Myanmar government in 2007 to establish a nuclear research center. The agreement calls for the construction of a 10MW light-water research reactor. The project was suspended over a destabilization in Myanmar following the Saffron Revolution and subsequent financial difficulties, including those associated with Hurricane Nargis. The political climate has since changed, and on September 17, 2013 Myanmar signed an additional protocol to its Safeguards Agreement with the IAEA under the Nuclear Non-Proliferation Treaty, meaning that the Rosatom contract might now prove easier to implement. Apart from the mining and power-generation industries, there are a host of opportunities on the Myanmar finance and credit markets for Russian financial and banking institutions, in particular for the state-controlled banks VTB and Sberbank. There is good reason to believe that the credit growth rate in Myanmar will stay very high in the near future, as is always the case for emerging markets.

The chances of Russian telecom specialists in Myanmar are also worth considering. In 2013, only 9 percent of the Myanmar population had access to mobile telecommunications, meaning that the sector is in for a huge boom very soon. Russian operators need to move fast: major European telecom providers are already expressing their interest in the market. Not to mention India and China, whose companies are already active in Myanmar. Procrastination would be perilous. In fact, the Russian telecom giant VimpelCom is already present in Cambodia, Laos, and Bangladesh. However, Russian companies should work closely with diplomats, lest they should run into problems like MTS did in India.39
Conclusion

business dialogue...
Notes
* The author is grateful to the officers of the International Cooperation Department at the
Russian Ministry of Education and Science for their kind assistance with the research.


2. The country changed its name to Myanmar in 1989 because this variant better
represents the native pronunciation and reflects the cultural and traditional
heritage of the country.


September 2013, ProQuest LLC, <http://search.proquest.com/docview/1428115017?

63347332690>, last accessed August 8, 2014.

6. Antony Collins, “Structural Obstacles Remain with Myanmar’s Emergence,” Project
Finance, May 2013, ProQuest LLC, <http://search.proquest.com/docview/1375639720?

7. AungHlaTun and Jared Ferrie, “Foreign Investment in Myanmar Surges, Office Rents
mar-investment-idUSL3N0HG0L420130920>, last accessed August 27, 2014.

8. Author’s interview with Yaroslav Lisovolik, Chief Economist of Deutsche Bank in Moscow,
Moscow, November 24, 2013.


10. Yulia Petrova, “Prices of Offices, Apartments Rise in Record-Breaking Short Time in
/v-myanmev-rekordno-korotkij-srok-podorozhali-ofsy#ixzz2jilxSPh>, last accessed August 27,
2014.

11. Elena Zubova, “One Hundred Years of Solitude: How to Make Money From Investment
243895-sto-let-odinochestva-kak-zarabatata-na-investitsiyonoi-likhoradke-v-myanme>, last

12. Ibid.


14. “Myanmar Faces Big Setbacks to Implement Stock Exchange, Says Deputy Minister,”
Eleven Myanmar, October 27, 2013, <http://elevenmyanmar.com/business/3871-myanmar-

15. AungHlaTun and Jared Ferrie, “Myanmar to Allow Foreign Banks to Begin Some

cash-in-myanmar-hard-to-displace-for-mastercard-visa.html>, last accessed August 27,
2014.


40 In February 2012, the Supreme Court of India revoked the license of the Russian telecom provider MTS, which resulted in significant reputational and financial losses for the company.


Amid the ongoing confrontation with the West, Russia’s foreign-policy course is pivoting towards the East, a region where new configurations of international alliances are being shaped, where integration institutes are evolving, and where the mechanisms of influence and cooperation are becoming more complicated.

For Southeast Asia, Russia still remains a guest whose strategic goals are unclear, but who is, nevertheless, aspiring to build closer bilateral relations in such areas as politics, economics, energy, science, and technology. Russia pursues a two-pronged approach to cooperation with Southeast Asian nations. On the one hand, it is trying to strengthen its positions in the Asia Pacific by stepping up its involvement in regional integration institutes and processes (such as APEC, ASEAN, and EAS) and various strategic dialogue platforms (ARF, the Asia-Europe Forum, ADMM-Plus, Asia Cooperation Dialogue forum, etc). On the other hand, Russia is also seeking closer cooperation and contacts on a bilateral level.¹

One of the key documents in the framework of Russia–ASEAN cooperation is the Intergovernmental Agreement on Cooperation in Economics and Development, which was signed in December 2005.²

On December 13, 2005 the two sides adopted a Comprehensive Action Program for 2005–2013. It is aimed at deepening and diversifying mutually beneficial cooperation between Russia and ASEAN nations.³ The program includes nine distinct areas of cooperation. Russia is particularly interested in military and technical cooperation, since the ASEAN markets account for up to 15 percent of global arms sales in dollar terms. The ASEAN nations also pursue long-term programs of modernizing their armed forces. Russia can also help ASEAN to diversify its energy sources, even though several of its members (Vietnam, Indonesia, Malaysia, and Brunei) are major producers of hydrocarbons. Finally, Southeast Asian countries are showing great interest in the latest Russian technologies in such areas as telecommunications, biotech, and space.⁴

Over the past decade Russia has also been trying to secure ASEAN nations’ interest in pursuing nuclear energy cooperation.⁵ Even though Russia is not the most significant actor in Southeast Asia, it has a significant strategic potential, advanced nuclear technologies, and world-class nuclear know-how. This attracts potential partners who are interested in peaceful nuclear energy.

NUCLEAR ENERGY DEVELOPMENT IN SOUTHEAST ASIA

There is a growing realization of the need to develop renewable technologies in Southeast Asia. Experts are worried by the prospect of growing carbon emissions as natural gas is being replaced by coal in electricity generation. This will significantly increase the environmental burden. As a result, researchers are predicting a deterioration in the environmental situation in Southeast Asia that will pose grave public health risks, slow the development of vital industries such as tourism, and destroy the region’s unique natural heritage.⁶
In Myanmar, proposals were made in the early 2000s to build nuclear power plants. Now, however, these plans are viewed as a matter of the distant future. At the time, it was Russia that was a potential source of nuclear power plants. In 2001, Moscow signed an agreement with Myanmar to build two nuclear reactors. Other experts argue that the first nuclear power plant should consist of two 1,000 MW reactors. Other options include the construction of smaller reactors, but this choice is difficult to make due to the size of the site.

Different opinions have been expressed regarding the size of the future reactors. Some experts believe that two reactors would be too small, while others argue that three would be too large. The final decision will depend on the economic and political situation in Myanmar.

In 2002, experts from the Atomic Energy Agency (IAEA) visited Myanmar to conduct a feasibility study. The IAEA recommended building two reactors, each with a capacity of 1,000 MW. The proposal to build two reactors was approved by the Myanmar government in 2004. However, the project faced significant challenges, including funding and technical issues.

The idea of building nuclear power plants in Myanmar has been criticized by international organizations, such as the International Atomic Energy Agency (IAEA). The IAEA has expressed concerns about the safety and security of nuclear facilities in Myanmar, and has recommended that the country prioritize the development of alternative energy sources.

In 2010, the government of Myanmar announced its intentions to build two nuclear reactors. However, the project faced opposition from environmental groups and local communities. The government has stated that the reactors will be built in a remote area, away from residential areas.

In conclusion, the decision to build nuclear power plants in Myanmar is complex and involves many factors. The government has stated that the reactors will be built in a remote area, away from residential areas, and that the project will be conducted in a transparent and responsible manner. However, the project faces significant challenges, including funding and technical issues, and there are concerns about the safety and security of nuclear facilities in Myanmar.

The government has stated that the reactors will be built in a remote area, away from residential areas, and that the project will be conducted in a transparent and responsible manner. However, the project faces significant challenges, including funding and technical issues, and there are concerns about the safety and security of nuclear facilities in Myanmar. The decision to build nuclear power plants in Myanmar is complex and involves many factors.
who approached Myanmar with a proposal to build a research reactor and a nuclear research center in the country.\textsuperscript{20} Russia had an opportunity to become Myanmar’s main nuclear energy partner, but the project was later frozen for political and economic reasons.\textsuperscript{21}

Singapore has shown interest in medium-size and small reactors, and said it was ready to cooperate with Malaysia in that area. In November 2010 Prime Minister Lee Hsien Loong officially declared that Singapore “cannot afford not to use nuclear energy”. Nevertheless, the small size of the city-state and its high population density mean that any man-made disaster would have very grave consequences.\textsuperscript{22} It seems unlikely that Singapore will build its first NPP any time soon.

The only country in Southeast Asia that has already built (but not launched) an NPP is the Philippines. The country’s first nuclear energy initiatives were launched under the Marcos regime and were largely spurred by the global energy crisis of 1973. The project to build the 621 MW nuclear power plant in Bataan was launched in 1976, and completed in 1984, costing the country’s treasury 460 million dollars.\textsuperscript{23}

After the overthrow of the Marcos regime in 1986 the nuclear power plant was mothballed. Almost 30 years on it has yet to be launched, largely because of unresolved financial and safety problems.\textsuperscript{24} The Chernobyl accident, which happened the same year as the Bataan NPP was mothballed, was a major blow for the project.

The arguments against the launch of the nuclear power plant include high seismic activity in the Philippines archipelago, even though the Australian consulting company MEETS says these fears are overblown (its researchers conducted various studies and found no substantial risks). Potentially a more serious obstacle is the lack of qualified specialists who could operate the NPP.\textsuperscript{25}

To summarize, among all the Southeast Asian countries, only Vietnam, Indonesia, and Thailand have detailed plans for nuclear energy development or have declared their intention to build nuclear power plants.\textsuperscript{26} Experts believe that nuclear energy development in the region will begin in earnest in the early 2020s, and that firm foundations will have been laid by 2030.\textsuperscript{27} At the moment, however, that process is still in the very early stages. As Svetlana Klyuchanskaya put it, “in most of these countries, nuclear infrastructure is being built from scratch…. As a result, the country that wins the contract to build a nuclear power plant is also likely to win contracts for training specialists for the future NPP, for maintaining the safety infrastructure, etc.”\textsuperscript{28}

On the whole, Southeast Asia has found itself between the rock of energy shortages and the hard place of risks (both avoidable and unavoidable) that are associated with nuclear technologies.

**CHALLENGES AND RISKS**

The public in those Southeast Asian countries that are planning to build nuclear power plants is concerned about the prospect of man-made disasters. In view of the region’s natural conditions and climate, such disasters could inflict irreparable damage to its wildlife as well as agriculture. (Nuclear power plants are usually built well away from big cities, even though people living in rural areas do not like that at all.) The rural population is usually opposed to any proposals to build a nuclear power plant in their area, regardless of the advantages of such projects trumpeted by the media and scientists. The public opinion in small towns and villages is often extremely intolerant of anything that has to do with nuclear energy, even though many of these negative expectations are unfounded, and there is no reason whatsoever for panic or alarmism. In fact, nuclear technologies can bring numerous benefits to agrarian regions. For example, the use of radiation can improve plant emergence and storability. Plant cells are less vulnerable to radiation; furthermore, radiation can make them more resilient without any harmful effects for the people who eat those plants.\textsuperscript{29}

Southeast Asian countries need to roll out social and education programs that help members of the public understand the real risks and benefits of nuclear energy, and to pursue awareness campaigns that emphasize the low environmental risks posed by modern nuclear technologies.
Inadequate level of individual training in the area of nuclear safety and security

- Lack of regulations and equipment for proper control, including insufficient use of I systems by the nuclear service
- Lack of regulations and control over nuclear facilities on the national level
- Lack of regulations and control over nuclear facilities in the nuclear sphere
- Absence of a truly independent nuclear regulatory agency
- Poor understanding of the concept of civil nuclear products

**Vietnam**
- Need to strengthen human resources in the nuclear industry
- Lack of resources to improve safety and security arrangements and culture

**Indonesia**
- Lack of resources to improve safety and security arrangements and culture

**Myanmar**
- Potential nuclear safety and security challenges in Indonesia, Vietnam, and Myanmar
- Limited potential nuclear safety and security challenges in Indonesia, Vietnam, and Myanmar
- Nuclear safety and security challenges in Southeast Asia, especially in view of increasing energy needs and the threat of terrorism. The situation in the region is exacerbated by the lack of adequate nuclear safety and security measures. Several key nuclear safety measures are lacking, including the development of a national nuclear safety strategy and the establishment of a national nuclear safety committee

**Indonesia**
- Potential nuclear safety and security challenges in Indonesia, Vietnam, and Myanmar

*Table 1. Potentially nuclear safety and security challenges in Indonesia, Vietnam, and Myanmar*
of regional and global economic processes. Southeast Asia’s huge strategic significance is based on its geopolitical situation and the growing threats related to social (man-made) and natural factors (tsunami, earthquakes).

Contradictions between Southeast Asian states that have different strategic potentials and military-political resources, but still try to prevent the strengthening of intra-regional actors, are not conducive to improving a climate of trust. Such a climate is an important prerequisite for developing nuclear technologies. In particular, the Philippines and Singapore regard prospects for building NPPs as one of the most high-profile political issues.  

Southeast Asian countries are especially worried by the high likelihood of China’s rapidly growing might eventually leading to an imbalance of power in the region. Such concerns have come to the fore once again in the conflict over the Spratly and Paracel islands in the South China Sea.

There is a good chance that peaceful nuclear energy programs in Southeast Asia will help to defuse tensions over the disputed islands and their oil- and gas-rich offshore areas. China is not opposed to nuclear energy development in Southeast Asia, provided that such development is pursued under IAEA supervision—especially since the region is part of the Zone Free of Nuclear Weapons agreed in the 1995 Treaty of Bangkok.

Building nuclear power plants will, however, require colossal financial resources, which Southeast Asian countries do not seem in a position to spend. Of course, there is a relatively cheap nuclear energy option in the form of floating nuclear power plants. Indonesia and Malaysia, as well as China, have already shown interest in this technology. For example, the Chinese want to position four such power plants in coastal areas of the South China Sea.

Such a step, however, would be fraught with potential political complications. Some experts have also expressed skepticism about floating NPPs. They believe that “the floating NPPs will be based on the KLT-40S reactors, which use highly enriched uranium.” Greenpeace specialists argue that a floating NPP reactor contains enough fissile material to build dozens of atomic bombs. In addition, experts are worried by the difficulties of providing adequate security measures for floating nuclear power plants.

At the same time, Southeast Asia has effective mechanisms of bilateral, multilateral, and regional cooperation that have become the basis of regionalization. The ASEAN Way format, meanwhile, has become an important platform for discussing the key problems facing the region. Another such platform is the ASEAN Regional Forum (ARF), which hosts discussions on security problems, threats, and challenges facing the region. At a meeting in Hanoi in 2010 foreign ministers adopted the Hanoi Action Plan, which focuses on active cooperation in fighting terrorism and transnational crime, maritime security, nuclear nonproliferation, and disarmament.

Four regional instruments have been created in the ASEAN framework that can be used to introduce and strengthen a program of physical protection of nuclear materials. They include the Treaty of Bangkok on a Zone Free of Nuclear Weapons; a regional agreement on cooperation in Asia and the Pacific; a regional IAEA project entitled Technical Cooperation Program; and the Forum for Nuclear Cooperation in Asia.

Brunei, Cambodia, the Philippines, Singapore, and Thailand participate in the Proliferation Security Initiative.

In 2005 Singapore began to hold regular Deep Sabre naval exercises to intercept ships carrying WMD and related technologies. Also, a nuclear forensic network is being set up in the region.

In September 2013 representatives of 41 countries took part in the first meeting of ASEANTOM (the ASEAN network of nuclear regulation agencies). Apart from the 10 ASEAN states, the organization also includes IAEA members. The new body aims to foster cooperation in nuclear safety and security, nuclear forensics, prevention of nuclear and radioactive smuggling, and facilitating the return of spent nuclear materials to their country of origin.

Five ASEAN states are members of ANENT (the Asian Network for Education in Nuclear Technology). The body strives to promote, manage, and preserve nuclear knowledge to ensure the continued availability of qualified human resources in Asia for the sustainability of nuclear technology.
WHAT CAN RUSSIA CONTRIBUTE?
WHAT CAN RUSSIA CONTRIBUTE?
projects, and Russia is currently planning to build 13 nuclear power reactors in the country, with a total capacity of 15GW.47

Speaking of the plans to build the Ninh Thuan 1 NPP, Russian Prime Minister Dmitry Medvedev has described them as “the flagship project,” and estimated its value at 10 billion dollars or even more.48 Vietnam remains one of Russia’s most promising nuclear energy partners in Southeast Asia.

Another relatively new project is Russia’s agreement with Bangladesh49 to build the Ruppur NPP, where two Russian-designed 1GW reactors are to be launched in 2020.50

In recent years Rosatom has also pursued contacts with the Institute of Nuclear Technologies in Thailand. Last year the two governments were drafting an agreement on cooperation in peaceful space exploration and a program of science and technology cooperation until 2020.

Rosatom Overseas is energetically promoting Russian nuclear technologies and products abroad, including in Southeast Asia. The company can draw on the expertise and capability of more than 250 Russian nuclear industry facilities. It offers unique and comprehensive energy solutions, from uranium mining to building energy grid infrastructure.51

On the whole, Russia has the capability to meet the most demanding requirements of its foreign partners as far as nuclear cooperation is concerned.

Apart from nuclear energy, Southeast Asian countries are also greatly interested in non-energy nuclear technologies (Table 2), such as using radioactive isotopes in medicine, agriculture, and other areas. Russia is in a very good position to meet these requirements, too.

Table 2. Use of radiation sources for non-energy industrial applications in Southeast Asia54

<table>
<thead>
<tr>
<th>Use of radiation sources for non-energy purposes</th>
<th>Vietnam</th>
<th>Cambodia</th>
<th>Laos</th>
<th>Myanmar</th>
<th>Thailand</th>
</tr>
</thead>
<tbody>
<tr>
<td>Irradiators</td>
<td>+</td>
<td>n/a</td>
<td>n/a</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Nuclear medicine</td>
<td>+</td>
<td>n/a</td>
<td>n/a</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Radio-isotopic diagnostics</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Radiotherapy</td>
<td>+</td>
<td>n/a</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Cyclotrons</td>
<td>+</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>+</td>
</tr>
<tr>
<td>Industrial radiography</td>
<td>+</td>
<td>+</td>
<td>n/a</td>
<td>n/a</td>
<td>+</td>
</tr>
<tr>
<td>Industrial instruments</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Reactor research</td>
<td>+</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>+</td>
</tr>
<tr>
<td>Neutron generator</td>
<td>+</td>
<td>n/a</td>
<td>n/a</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Radioactive waste disposal</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Use of radiation sources for non-energy purposes</th>
<th>Indonesia</th>
<th>Philippines</th>
<th>Brunei</th>
<th>Malaysia</th>
<th>Singapore</th>
</tr>
</thead>
<tbody>
<tr>
<td>Irradiators</td>
<td>+</td>
<td>+</td>
<td>n/a</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Nuclear medicine</td>
<td>+</td>
<td>+</td>
<td>n/a</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Radio-isotopic diagnostics</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Radiotherapy</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Cyclotrons</td>
<td>+</td>
<td>+</td>
<td>n/a</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Industrial radiography</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Industrial instruments</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Reactor research</td>
<td>+</td>
<td>+</td>
<td>-</td>
<td>+</td>
<td>-</td>
</tr>
<tr>
<td>Neutron generator</td>
<td>+</td>
<td>+</td>
<td>n/a</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Radioactive waste disposal</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
</tbody>
</table>

Note: n/a = information not available.
Every threat to stability in Southeast Asia can also lead to conflict in the region. Nuclear energy is one of the most promising areas for cooperation in Southeast Asia. Russia and Southeast Asian nations must take into account the region’s specific environmental and geopolitical conditions.

**Conclusion**

Cooperation programs between Russia and Southeast Asian countries must incorporate nuclear energy development and promote nuclear security.

**Notes**

*The words “energy” and “nuclear” are underlined in the document, indicating their importance.*
12. Desker, op. cit.
15. Desker, op. cit.
23. Klyuchanskaya, op. cit., p. 70.
27. Desker, op. cit.
28. Klyuchanskaya, op. cit., p. 64.
29. Interview with the head of the Far Eastern Science and Education Center of Nuclear Technologies and Radiation and Ecological Safety, D.G. Kryukov, Vladivostok, Russia, July 17, 2014.
31. “Prospects for Nuclear Security in Southeast Asia,” prepared by the James Martin Center for Nonproliferation Studies (CNS, Monterey, United States), the Center for Energy and Security Studies (CENESS, Moscow, Russia), and the Vienna Center for Disarmament and Non-Proliferation (VCDNP, Vienna, Austria). Monterey/Moscow/Vienna, May 2012, pp. 16-17.
OUTCOMES OF THE RUSSIAN–U.S. HIGH-LEVEL WORKING GROUP ON THE IRANIAN NUCLEAR ISSUE

The Russian–U.S. working group on the Iranian nuclear issue was established in November 2013 by the PIR Center a leading Russian NGO in the area of international security, and the Near East South Asia Center for Strategic Studies (NESA), a regional center under the U.S. Department of Defense. The aim of the group was to support the positive dynamics of the process of negotiations between Iran and P5+1 and contribute to reaching of the Comprehensive Agreement on the Iranian nuclear program.

The meeting of the group took place in Gstaad, Switzerland on January 27–29, 2014. It was later supplemented by the coordinators’ work in May of 2014.

***

PROJECT COORDINATORS’ SUMMARY

1. NEGOTIATING THE FUTURE OF THE IRANIAN NUCLEAR PROGRAM UNDER THE COMPREHENSIVE AGREEMENT

1.1. The manner of implementing the Interim Agreement will shape the negotiations on a permanent agreement.

1.2. The majority of the members of the group agreed that there is a 6- to 12-month window of opportunity to reach agreement with Iran. Therefore the first priority should be given to the measures that could be implemented and bear fruit within this time limit.

1.3. All members of the group agreed that the Arak heavy water research reactor should be converted into a light water one or modified in order to produce less plutonium. No reprocessing facilities should be constructed in Iran.

1.4. The majority of the members of the group agreed that Iran should ratify an Additional Protocol to its IAEA Comprehensive Safeguards Agreement, and start applying modified code 3.1 of the Subsidiary Arrangements General Part to the country’s Safeguards Agreement.

1.5. All members of the group agreed that Iranian ratification of the Comprehensive Nuclear-Test-Ban Treaty and enabling the work of the monitoring stations could be a good confidence-building measure and should be encouraged. Some members of the group believe that Iranian ratification is only possible and meaningful with parallel voluntary ratification of the CTBT by Egypt and Israel.

1.6. All members of the group agreed that Iran should be encouraged to ratify the Convention on Nuclear Safety, the Vienna Convention on Civil Liability for Nuclear Damage, and the Convention on the Physical Protection of Nuclear Material.

1.7. The majority of the members of the group agreed that the limitations on the Iranian nuclear program that go beyond the NPT should be aimed at showing the peaceful nature of the program and will not be permanent. Some members of the group
Some members of the group believe that the only way to deal with current sanctions is to strengthen existing ones, instead of against Iran (both international and unilateral) would be their suspension instead of

2.1. All of the members of the group believe that the comprehensive agreement with Iran is considered those should be no new nuclear-related sanctions imposed on the country, because it would be a mistake and could break the negotiating process.

2.2. All of the members of the group believe that new nuclear-related sanctions should be lifted, once the regime of Syrian President Assad is overthrown, which is considered a sign that the nuclear program will be stopped.

2.3. The majority of the members of the group agree that the US-related sanctions against Iran should be lifted, once the regime of President Assad is overthrown.

2.4. The majority of the members of the group agree that sanctions relief will provide to be one of the most difficult parts in reaching and implementing the agreement. As the sanctions relief should be passed prior to reaching such an agreement.

2.5. Might consider the benefits of the process and go along with it.

2.6. Some members of the group believe that the only way to deal with current sanctions is to strengthen existing ones, instead of against Iran (both international and unilateral) would be their suspension instead of
removal. The suspension would require yearly renewal conditioned by certification that Teheran is not involved in illicit nuclear activities. Such a mechanism would have better chances of passing through the U.S. Congress.

3. ENGAGING IRAN

3.1. Some members of the working group stressed that the Geneva agreement remains very fragile and became possible because of the unified position of P5+1. All the actions that could provoke tensions between the members of the group (e.g. introducing new sanctions against Iran, circumventing the current sanctions regime) and undermine the negotiating process should be avoided.

3.2. Some members of the group proposed a greater engagement with Iran within the IAEA International Project on Innovative Nuclear Reactors and Fuel Cycles (INPRO). In the format of INPRO Iran could be advised on the best energy mix and on the building of its nuclear plants. Russia and the United States could both participate in this process.

3.3. Some members of the working group noted that the core of the Tehran research reactor is obsolete and should be replaced with technical assistance from the IAEA, Russia, and the United States.

3.4. Some members of the group indicated that organizing nuclear safety and nuclear security exercises in the Middle East with Iranian participation (those might include Bushehr NPP stress tests) could help reduce fears of Iran’s neighbors and decrease tensions in the region. Some experts believe that Iran should be invited to the next Nuclear Security Summit in Washington in 2016.

Some members of the group find it necessary to aim, in the long term, at implementation of joint programs (by Russia, the USA, or both) in the nuclear sphere in the Middle East with Iranian participation. Those programs should be economically viable and demonstrate the transition from confrontation to the cooperation in the region.

3.5. Some members of the group noted that Iran does not have enough natural uranium for a nuclear program on its territory. Contracts for shipment of natural uranium under strict international monitoring will be seen as a sign of good will in the negotiations.

3.6. Some members of the group proposed to elaborate on the opportunity of the United States buying enriched uranium for its nuclear power plants from Iran. This would play well with Iranian pride, and shift the relations between the two countries from politics and ideology to the economy. Being a customer could give the United States the possibility to put forward some recommendations and conditions when it comes to uranium enrichment.

3.7. Some members of the group noticed that while engaging Iran in technological cooperation might have benefits, sensitive technologies must not be shared.

3.8. Some members of the group believe that there is a need for close cooperation with Iran to help move the country off the Financial Action Task Force on Money Laundering (FATF) black list and for step-by-step reintegration of Iran into the international financial system.

3.9. Some members of the group proposed to help to accelerate Iranian accession to the World Trade Organization.

4. REGIONAL DYNAMICS

4.1. To date, other Middle East countries have not been invited to the table to negotiate the Comprehensive Agreement. It seems that this will be a prevailing trend: to isolate the nuclear and the regional tracks.

4.2. At the same time the very process of trust-building between the P5+1 and Iran caused some significant shifts in regional politics (e.g. in relations between Iran and Saudi Arabia, Iran and Israel). Countries of the region could be further engaged in the process of normalization of relations; they can also play a role in a Comprehensive Agreement. Third parties could provide technical support for implementing and verifying the provisions of the agreement. There are a number of states that have
NOTE

Some members of the group proposed that Russia and the United States, as well as powers, so many commitments in the Middle East in order not to be outpaced by the regional agreements. To support these efforts, the United States should pursue active engagement in the region with regional allies in the region to negotiate a regional agreement, to cooperate with the IAEA. Some members of the group argued that a regional agreement would be more difficult, primarily due to thevarious approaches to the issue of nuclear weapons. The agreement could be initiated by negotiations under the IAEA framework, or through the UN Security Council. This would make negotiations more difficult, and produce incentives for all countries of the region. Some members of the group proposed reaching a comprehensive agreement with Iran.
A year after the 2013 APEC summit in Vladivostok, Southeast Asia retains and enhances its appeal to Russia as a promising platform for growing trade and economic ties. At the same time, against the backdrop of growing contradictions with the West and the ongoing process of new global power centers coming into their own, regional players in Southeast Asia—and especially ASEAN—are becoming increasingly important partners in the foreign policy dialogue. Within such a dialogue, a wide range of issues is coming to the forefront of the cooperation agenda, including the problems of regional security and global security. What problems lie at the intersection of these two large baskets in the Russia–ASEAN foreign policy dialogue?

The study of this issue has led the PIR Center and invited Russian experts to the conclusion that one of the most popular and promising, though obviously challenging and highly competitive potential areas of cooperation between Russia and ASEAN countries is the information technology (IT) sector. On the initiative of the PIR Center, representatives of government, business, and the technical community and academe made an effort to identify the common interests of Russia and the ASEAN states with regard to strengthening global security in cyberspace, and also to evaluate the potential of Southeast Asia as a market for Russian information security products and services, and additionally as a hardware manufacturing site for Russian companies. Another issue on the agenda was the pros and cons of Russia adapting the ASEAN experience in the establishing of effectively functioning networks of Computer Emergency Response Teams (CERTs) and fighting transborder cybercrime with the help of private companies and their resources.

The discussions and workshops organized by the PIR Center were attended by leading Russian experts in the field of information security, including the Expert of the Department of New Challenges and Threats at the Ministry of Foreign Affairs of the Russian Federation Boris Vasiliev, Deputy Head of Computer Incident Response at Group-IB Alexander Kalinin, Information Security Business Consultant at Cisco Systems Aleksey Lukatsky, Chairman of the Board at the Coordination Center for the Top Level Domains .RU/.FE Mikhail Medrish, the PIR Center President Vladimir Orlov, Executive Director of the Russia–ASEAN Business Council at the Chamber of Commerce of the Russian Federation Viktor Tarusin, member of the PIR Center Board Michael Yakushev, and the Head of Strategic Projects at the Kaspersky Lab Andrey Yarnykh.

UNITED BY A COMMON THREAT: DISCUSSION OF CYBER ATTACKS AND TRANSBORDER CYBERCRIME IN RUSSIA AND ASEAN

YARNYKH: I would like to highlight the issues of cyber-warfare and contemporary cyber threats, particularly with regard to the ASEAN region.

First, some historical perspective. In 1994, Kaspersky Lab experts detected an average of one virus per hour, and at the time we mostly did not require complex machine analysis and the data scanning in search of malware. In 2006, new viruses were detected every minute; this required automated analytics, and we began to fight viruses using robot programs. By 2011, new samples of malicious code were detected by our experts each second. At these
officer espionage involved by strategic and political ends.

The cyberespionage threat over the globe, including Russia and the ASEAN region, is a growing threat to the world, affecting businesses and governments. A recent study of the extent of espionage activities showed that 15% of targeted organizations were engaged in diplomatic activities. Around the world, diplomatic offices are the targets of espionage activities, including those of the US, China, and Germany, among others. This is a significant issue in both countries, as seen in the case of China and Russia, where the threat is severe.

In the ASEAN region, the threat is significant, with the cyberespionage activities targeting the region's critical infrastructure. The threat is especially severe in the oil and gas sector, where the cyberespionage activities are aimed at stealing valuable information and intellectual property. This is a significant issue, as the region's oil and gas industry is vital to the world's energy supply.

The cyberespionage activities are not limited to the oil and gas sector, as seen in the case of Malaysia, where the threat is severe. The Malaysian government is taking steps to combat the threat, including the establishment of a national cyber security center. However, the threat is still significant, and more needs to be done to ensure the protection of critical infrastructure.

In conclusion, the threat of cyberespionage is significant, and governments and businesses need to take steps to protect themselves. This includes the establishment of national cyber security centers and the implementation of robust security measures. By taking these steps, we can ensure the protection of critical infrastructure and the safety of the global economy.
Such trends are really dangerous and unacceptable. Cyber weapons should be prohibited for use globally; otherwise, our networks and devices will become a breeding ground for their further development and dissemination. Kaspersky Lab has been calling for such measures for a long time and so far all the trends of malware evolution that we observe prove the relevance of our proposals. The ASEAN region is by no means an exception from the global picture, so I think that countering the use of cyber weapons might be a good topic for Russia–ASEAN cooperation in the nearest future.

KALININ: I would like to add to what Andrey Yarnykh said and briefly highlight the spectrum of cyber threats in the ASEAN region that my company, Group-IB, faces within its own business niche—the segment of cyber-incident response and computer forensics. Since 2011, Group-IB has been publishing an annual report on the development of the global cybercrime market, and each year the final figure grows. In 2010 it amounted to $7 billion, while in 2012 it was already at $18 billion. A considerable share of this huge sum of money was generated by actions affecting or concerning Russia and, to an equal extent, the states of Southeast Asia.

In addition to attacks on individual users, a huge number of attacks on corporations are originated from within the territory of the ASEAN states. Even a shortlist of the origins of the most massive and sophisticated attacks includes Malaysia, Thailand, the Philippines—in sum, at least half of the ASEAN countries. Such incidents as the execution of malicious code on a company’s servers and the scanning of corporate networks occur on a regular, systematic basis, and in order to prevent them we cooperate with dozens of countries. As a rule, representatives of private enterprises and public agencies that find themselves under such attacks need to know what is happening, and they regularly submit reports on the steps they have taken to ensure cybersecurity, block malicious resources, or apply sanctions against the actors who carry out these attacks.

Let me mention one example from Group-IB practice: a high-profile cybercrime case that concerned prevention of the activities of a cybercrime group that created and distributed bundles of exploits that took advantage of vulnerabilities in popular web browsers. To infect devices successfully, the criminals applied several zero-day vulnerabilities that were never previously used or discovered. The members of the group, a total of about 13 people, were apprehended in November 2013. A court verdict in the case is still pending, but the criminals certainly could be sentenced to 5–10 years of imprisonment. It should be noted that, while active, they inflicted damage valued at 70 million rubles—and this figure only reflects the episodes revealed in the process of investigation and confirmed by collected evidence.

Significantly, the capture of the cybercriminals would have been impossible without the collaboration with colleagues from the ASEAN region, including specialized governmental agencies in Malaysia. That collaboration was no coincidence—if one had a look at the control panel of the exploits disseminated by this cybercrime group, one would have seen that their geography covers many ASEAN countries. In this regard, Group-IB received a lot of support: upon our request, the data were disclosed on the registration of websites used for the implementation of fraud, information regarding the sources and purposes of attacks, as well as other information that led us directly to the authors of these exploits.

I would like to support Mr Yarnykh and to emphasize that, despite the permanently growing supply and technological sophistication of the global cybercrime market, there is a parallel expansion of opportunities for cooperation between Russia and other countries and organizations, such as ASEAN, to effectively counter those threats. But, of course, a great deal still remains to be done.

THE GLOBAL GOALS FOR RUSSIA AND ASEAN: PREVENTION OF CYBERWARS AND ENSURING SECURITY IN CYBERSPACE

ORLOV: Our discussion today is two-pronged; it highlights cyber threats common to Russia and ASEAN countries, as well as shared perspectives for trans-regional cooperation in this field. Previous speakers elaborated in sufficient detail on the spectrum of threats, which equally affect Russia and Southeast Asia. However, apart from cybercrime, cyber espionage and cyber terrorism, we cannot fail to mention other threats, such as military and political ones. Moreover, the region’s countries cannot remain isolated from the global Internet
Building measures in cooperation with ASEAN countries to strengthen the ASEAN cooperation-building mechanism and the implementation of practical initiatives in the field of cybersecurity. This is a multi-year project, and cybersecurity cooperation-building measures remain a challenge.

The Belt and Road Initiative. We know that our cooperation within the ASEAN region is particularly relevant in the context of China’s Belt and Road Initiative. China is a member of ASEAN, and we support its cooperation with the ASEAN countries, which is necessary for the economic and political development of the region.

In conclusion, we affirm the importance of cooperation within the framework of ASEAN and the Belt and Road Initiative, which is relevant for the development of our region and the global community.
geographically beyond the boundaries of ASEAN, as well as outside the format of the SCO—which could yet be more effectively engaged in cooperation. I would be happy to receive comments from colleagues on my observations.

LUKATSKY: Indeed, the potential areas of common interests between Russia and the ASEAN countries have to do primarily with the fight against cybercrime and cyber terrorism. However, we also should not overlook the opportunity to use the boosting of ASEAN markets to promote Russian technologies and Russian products and services in the field of information security. As far as this is concerned, we have quite a positive experience. In addition, there is a chance to use Russian experience in the elaboration of hardware and creating assembly sites for products that could then be used in certain critical areas.

In Russia, some nuances have come into stark relief over the last two years. They were to some extent related to the Snowden effect, but mostly they just reflect the peculiarities of regulatory policies imposed by the Russian governmental agencies in charge of the information security issues. So it will not be so easy to reallocate outside of Russia an entire production cycle of elements used in critical information infrastructure. Another area of potential cooperation is the elaboration of doctrinal and strategic documents on information security issues, including national information security and cybersecurity strategies.

Since 2000, the Information Security Doctrine of the Russian Federation has served as the official cornerstone of the national approach to the issues of information security. However, today there are different perspectives towards this document. Technical experts from the IT sector tend to opine on the obsolescence of the document. The Doctrine does not reflect the actual conditions and the present-day situation in this field, which is very dynamic; to conduct policy based on 14-year-old documents is no longer possible. Largely in response to this problem, in September 2012 the Russian Council of Federation set up an expert group that launched elaboration of a draft concept of Russia's national cybersecurity strategy. By the end of 2013, the draft document was at a very advanced stage, but in the course of parliamentary hearings on the draft in the Federation Council, held on November 29, 2013, outcomes of our work met quite serious criticism, which was focused primarily on terminological aspects. Again the question arose as to why the draft document used the term "cyber security," instead of "information security." It also became evident that there was no clear understanding on what place the draft Strategy would hold among other doctrinal documents encapsulating Russia’s approach in the field of information security, national security, foreign policy, etc. On December 10, 2013, there was another meeting on the draft Strategy, where these questions were put forward. Today, a year later, the fate of this draft document remains unclear. It does seem that the draft concept of the Strategy met opposition from a number of government agencies, although its provisions seem quite sensible and timely.

In this regard, Russia might be interested in the experience of ASEAN countries, particularly Singapore, which as early as July 2013 published the third version of a similar document, the five-year National Cyber Security Masterplan 2018 (NCSM 2018). Since 2005, Singapore has released such documents every five years. The latest edition reflects all the key issues that were mentioned in the draft concept of Russia’s National Cybersecurity Strategy of 2013. This includes issues of raising awareness and information sharing, public–private partnerships (PPPs), international cooperation, as well as the issues of training education, increasing the number of specialists in this area, and development of a network of governmental and private CERTs.

YAKUSHEV: I would like to draw attention to the issues of terminology. Last year demonstrated considerable though unexpected progress in the terminological debate on security in the use of ICTs between Russia and the United States, one of the principal opponents of Russia in this area. On June 17, 2013, on the margins of then G8 Summit in Ireland, Barack Obama and Vladimir Putin signed a set of agreements putting forth a system of mechanisms for development of bilateral confidence-building measures aimed at preventing security threats coming from cyberspace. This compromise might prevent further disputes on issues of terminology in the field of information security. Unfortunately, the deterioration of bilateral relations in the context of the Ukrainian crisis today leaves almost no chances for successful development of these mechanisms now. Still, the very precedent of this collaboration is very positive, and the initial set of mechanisms and CBMs should be
thoroughly studied, and then probably developed and applied for some new frameworks, ASEAN as a possible option.

Second, it is also important to understand to what extent we and our colleagues in the ASEAN region coincide in our visions of the cyberspace assets that should be protected in first place. First and foremost, this is about critical infrastructure protection. Third, there is a variety of ways to mitigate cyber threats, including legal, institutional, and technological mechanisms and practices. It would make sense to use the extensive and longstanding experience of Russian diplomacy, the information security industry, and the expert community for further development and enhancement of these instruments in the ASEAN region.

Finally, the issues of information security are closely linked to the issues of global Internet governance, and the oversight of the Internet's critical resources. These issues became especially topical after the disclosures of global governmental online surveillance programs disclosed by Edward Snowden in 2013. It would be interesting to hear the expert opinions on how these issues are seen now, one year later.

VASILEV: To give an idea of the priorities of the Russian approach to information security, including cooperation with the ASEAN states, I would like to mention some of the key Russian documents in this field. In August 2013, Russian President Vladimir Putin signed the Basic Principles for State Policy of the Russian Federation in the field of International Information Security to 2020. This doctrinal document sets the directions in which we move forward, and enumerates all major threats in this area and various ways to counter them, including a number or tracks and formats for international cooperation that we consider priorities. The document highlights several key types of threats to international information security, and puts emphasis on the fundamental "Triad of threats," which encompasses the use of ICTs for military and political, terrorist, and criminal purposes.

However, apart from this basic classification, the document introduces a new, fourth type of threat: “interference in the internal affairs of sovereign states, violation of the public order, incitement of ethnic hatred, racial and religious enmity, propaganda of racist or xenophobic ideas or theories that give rise to hatred, discrimination, or incitement to violence.” This is an interesting and important point, because the threat is new and did not appear previously in doctrinal documents, although now we must take it into account. It is also important that the Basic Principles for State Policy put cooperation with regional associations and organizations into the rank of major priorities with regard to international cooperation on these issues. Among the key regional formats, such as the SCO, BRICS, and the Commonwealth of Independent States (CIS), the ASEAN Regional Forum—ARF—is also mentioned in the first lines.

From here, I would like to comment briefly on Dr Orlov’s remarks, which in fact provide almost a complete description of the work being done within the framework of the ARF on the issue of information security. One minor elaboration refers to the ARF work plan on security in the use of ICTs. Starting in 2012, the Australian side initiated elaboration of such a plan, as one of the co-chairs of the process alongside Russia and Malaysia. In 2013, the Australians submitted the draft document; further work on it aimed to reflect critical remarks introduced by the two co-chairs, Russia and Malaysia. In November 2013, the proposals developed by Australia and other interested parties were summarized in a preliminary Draft Plan; on the initiative of the Australian side, the draft document was presented on December 9–10, 2013 in Myanmar, at a meeting of the ARF Inter-Sessional Support Group. In 2014, further harmonization of the draft document with the views of the Russian side followed. This process should be completed before the end of 2014. In this work we fully support Malaysia as the third co-chair of the Work Plan elaboration process.

Active discussion on international information security has been underway in the ARF framework. On September 11–12, 2013, Beijing hosted the First ARF Workshop on Cyber Security which considered, inter alia, the legal and cultural aspects of cooperation in the field of the use of ICTs. The Workshop was co-organized by China and Malaysia, and was attended by experts from 19 countries—members of the ARF as well as representatives of the European Union and the ASEAN Secretariat. On aggregation of the reports, presentations, and discussions at the seminar, two major approaches towards international information security crystallized. According to the first, which is mostly promoted by the USA, there is no need to restrict or legally prohibit the use of ICTs for military and political purposes; instead,
proper regulation and interpretation of such activities should be discussed and elaborated. In such a case, these regulations should be based on the existing law, so there is no need to adopt new norms or legally binding international agreements.

We have criticized this approach; and we are promoting our own alternative, which implies establishment of an international legal regime that would prohibit the use of ICTs for military and political purposes.

In principle, the two approaches together encompass a range of positions that could serve as a guide to any country. Russia has been acting in concert with China, which generally supports our approach, aimed at ensuring the security of our society and the state. As for our Western partners, they want to ensure their security when using IT for military and political purposes against third parties; as far as we can see, this motivation is clearly identifiable in the approach of the West.

At the moment, almost every state is capable of delivering an adequate response to a cyber attack conducted against it by another country. Therefore, when attacking even a weak country, a strong cyber power should take into account the probability of a counter-strike.

The reason for this is that one does not need any unique resources or extremely advanced technologies in order to inflict serious damage to critical information infrastructure objects and the country’s reputation. Hence, it is understandable that Western countries want to retain the ability to use ICTs for military and political purposes, as a kind of deterrence mechanism that would not allow weaker nations to respond to such actions in a symmetric way.

**CAPITALIZING ON COOPERATION: PROSPECTS AND INTERESTS OF THE IT SECTOR IN THE ASEAN MARKET**

**TARUSIN:** The ASEAN market today presents a situation quite advantageous for major actors in the Russian IT sector. Against the backdrop of the 2013 events related to the disclosures made by Edward Snowden, the U.S. companies which are the key competitors of the Russian information security businesses have considerably lost trust in the eyes of their customers, including potential ones. According to independent estimates, the damage from these events to the U.S. IT sector through 2020 could be as high as $35 billion. This opens up an opportunity that Russian information security software vendors could exploit, replacing their American counterparts to a certain extent. ASEAN countries currently make up a substantial part of the global market for IT products, and now we need to take advantage of this opportunity and intensify the efforts of the Russian companies aimed at entering these markets.

In the second half of 2013, Russian IT companies saw an unexpected surge in demand for their products in unusual regional markets. For example, at the Mail.ru portal, which registers 30–40,000 new e-mail addresses daily, 70% of the applications received in the second half of 2013 originated from the Middle East. This trend is illustrative, and I think that, if Russian interests and capabilities are properly aggregated and promoted, ASEAN customers could also switch to Russian IT solutions on a massive scale. One cannot argue that Russian information-security companies are the only alternative to Western corporations in ASEAN markets.

There is very serious competition from Chinese companies, especially in the information security segment. Nevertheless, the possibility and necessity of accelerated activities in the regional market on the part of Russian business enterprises is not in doubt. Once again, I take this opportunity to draw the attention of all stakeholders of the IT industry to the positive experience of the business mission of Russian entrepreneurs to Southeast Asia, which took place on 22–30 March 2014, jointly with the Ministry of Economic Development and the Ministry of Foreign Affairs, and covered three countries: Indonesia, Malaysia, and Singapore. Senior governmental officials and business leaders attended the events conducted as part of the mission from the three countries. I believe that with actions, and similar missions, we could really demonstrate our interest, and—most importantly—highlight the capabilities of Russian companies to provide high-quality competitive products and services.
LUKATSKY: With regard to Russian business prospects in the ASEAN information security market, we would be talking about promotion of Russian information security software and hardware solutions to the markets of the Southeast Asia. We already have considerable experience in this area: this would be Kaspersky Lab, as well as Doctor Web, and Positive Technologies, which either have representative offices in Southeast Asian states, or sell to customers in the region from neighboring countries. At the same time, in 2013 these companies faced aggressive competitive policies on the part of Chinese companies, which are geographically closer, and boast stronger cultural and commercial ties in the region’s market compared with Russia. Because of these specific advantages, Chinese businesses are able to work with customers in the ASEAN countries in more subtle, precise, and focused ways, while Russian companies face ostensible though not insurmountable difficulties.

Also of interest is the fact that the marketing positioning of the information security vendors does not imply distinctive national identity. In spite of the Snowden effect, already mentioned today, as a representative of the U.S. company Cisco Systems, I cannot say that we witnessed a strong slide in our sales in the regional markets over 2013. Much depends not on the nationality of a company, but rather on the attitude that a transnational corporation shows toward a certain market. I am talking about the possibility of working with federal regulators, and the ability to ensure the compliance of specific information security products with the governmental requirements in certain countries. In this regard, Russian products in the field of information security have every chance of entering the ASEAN market. Similarly, Southeast Asian companies could effectively move their IT products to the Russian market.

At the same time, the Russian regulatory market for information security products is quite peculiar and differs from those models that work beyond Russia’s borders. For instance, in Russia specific requirements are in place with regard to security compliance assessment. Such requirements include mandatory provision of the product’s source code, which is quite challenging for many foreign companies. One of the reasons for refusal are concerns over their intellectual property rights and their protection. In 2013–2014, the disclosures made by Edward Snowden showed Russian companies how they could use this to their advantage. I cannot make claims with regard to Southeast Asia, but in the second half of 2013, the Arab countries began to turn away from American IT products—at least in the field of cryptography—and look at solutions developed in Russia. As a result, a certain upsurge of interest in Russian cryptographic algorithms and Russian encryption products could be seen in the Arab world. This is an interesting trend, and we could try to take advantage of it.

Another issue is production of hardware in the countries of Southeast Asia. If we consider the mainstream end-user market of IT products, no specific issues or challenges arise. But if we are talking about segments related to information security, then, unfortunately, we should keep in mind that recent trends, such as the increase in massive cyber attacks and incidents, the Snowden revelations, etc. create a situation where no country wants to outsource the production of critical infrastructure components outside of its borders, even regardless of the guarantees of 100 percent control of the technological processes at foreign facilities.

This trend is obvious in the United States, which is reallocating part of its production in the information security hardware sector from Southeast Asia and China back to national territory. A similar trend exists in Russia. Government regulators are reluctant concerning the idea of production of the hardware components of critical systems anywhere abroad; Southeast Asia not an exclusion. In fact, this logic pertains in other regions as well, including Europe. Today each country wants to manufacture and assemble key hardware components of its IT systems on its own territory under its own control. Thus, Russia probably does not have great prospects in this niche, as far as the ASEAN region is concerned. However, this is certainly not the case with the mass end-user market, so we should probably try to take a chance there.

TARUSIN: Further to the comment by Alexey Lukatsky, I would like to explain precisely why at the moment ASEAN looks so promising for Russian IT products as a regional market. First, ASEAN today is among markets demonstrating the most rapid and stable growth. Against the backdrop of global economic catastrophes, which we have witnessed in the United States and Europe over the past years, the ASEAN economies seem to be remarkably dynamic and promising, making up what is essentially a single economic mechanism. Second, the deteriorating crisis of our relations with the West encourages us to seek opportunities in
those markets where the risk of sanctions and other restrictive mechanisms for Russian products is incomparably lower.

For 2015, there are plans to establish the ASEAN Economic Community (AEC) with a single market, which would create a genuine free-trade zone, supported by additional administrative measures, such as a single visa for ASEAN states. Implementation of this idea will remove many barriers to further development of trade cooperation. ASEAN boasts a population of 600 million and a potential gateway for Russian industrial products to the consumer markets of at least 10 countries. Unfortunately, in 2013, the total volume of trade between Russia and ASEAN countries was just over $15 billion. Most of this trade is in energy and raw materials, such as palm oil and natural rubber.

At the same time, there are breakthroughs and success stories associated with the IT segment. When in 2012 the Deputy Secretary-General of ASEAN, Dr Lim Hong Hin, asked me to name at least one charismatic, recognizable Russian entrepreneur doing business in the ASEAN countries, I instantly named Eugene Kaspersky and his company—because it is indeed Russia’s face in the region. All we need to do is to competently use this springboard to move into related industries and segments, to consolidate and increase Russia’s presence in the region. It is important to promote not only off-the-shelf products, which are already easily recognizable in Jakarta, Colombo, Kuala Lumpur, and Hanoi—but also corporate solutions, where we can seriously compete with businesses from other countries. That is why the Russia–ASEAN Business Council has been making every effort to promote Russian high-tech products to the ASEAN market. To date, we represent over 20 companies, many of them specialized in the field of information security.

We try to use our framework to allow the representatives and heads of these enterprises to speak directly to the business sector in the ASEAN countries. In June 2013, in St Petersburg, we conducted the first Russia–ASEAN Business Forum, and invited prominent business leaders such as Natalya Kaspersky, CEO at InfoWatch, and Anatoly Klepov, one of the leading experts on information security. Presentations and reports highlighted the issues of information security of the mobile networks, as well as enterprise networks, and the banking sector. In addition, we used the financial support mechanism of the ASEAN–Russia Dialogue Partnership and launched two initiatives that would allow our members to present their products to the ASEAN Secretariat and to ASEAN businesses. The list of such products includes unified electronic-trading platforms, and an interactive investment portfolio that can be seen in the Google Store, in the public domain.

I also want to draw attention to the fact that ASEAN is a peculiar market for us. With the European mental patterns typical of Russians, it may be very difficult to grasp some of its peculiarities. When you come to ASEAN markets with something new, which you believe is most important and necessary for the region, the first thing you will be asked is, “Who will invest in the project?” We started addressing this problem in cooperation with the Russian Ministry of Economic Development in 2013. We have an agreement with the Minister Alexey Ulyukaev, which is also strengthened by support from the Russian Direct Investment Fund (RDIF).

Last but not least, we are creating a fund to support Russia–ASEAN investments, which, among other things, would be aimed at promoting Russian products to 10 countries in the region, including Russian high-tech solutions. With such a mechanism, we would be able to achieve a significant breakthrough in the regional IT market. On one hand, we expect that the representatives of the private sector will be able to benefit from the synergies with the Fund to promote these products to the regional markets. On the other hand, we believe that Russian business leaders will help us to fill this fund with concrete products that would be not at the start-up stage, but ready to be launched into full-scale industrial and commercial production. Let us hope that our ambitious plans will become a reality.

EXCHANGING INFORMATION AND RESPONDING TO INCIDENTS: THE ROLE OF CERTs IN RUSSIA–ASEAN COOPERATION IN CYBERSPACE

LUKATSKY: Within the entire spectrum of potential cooperation between Russia and ASEAN in the field of IT, there is an important niche within which we would really cooperate very actively, including from the point of view of learning from the experience of ASEAN countries.
We are talking about the development of mechanisms for CERTs and CSIRTs—special groups or teams that respond to cybersecurity incidents and threats that can come from any country or place in the world. And if in Russia today there are formally four CERTs, the ASEAN countries, whose territory and population are smaller that Russia’s, altogether have about 30 such teams. One example is the Asia-Pacific CERT (AP-CERT), a mechanism uniting 30 teams from 20 countries in the region. AP-CERT not only offers a set of services to commercial organizations or government agencies, but also publishes useful information on software vulnerabilities in the information systems, so that stakeholders could resolve problems in a timely manner and avoid serious incidents.

Another remarkable practice that Russia has not yet adopted is cybersecurity training; this format that was originally tested in Australia in the early 2000s. The Australian experience was then adopted by the United States, the EU, and the ASEAN states. This format allows for the elaboration and enhancement of formats to collaborate and methods to mitigate the threats of cybercrime, cyber terrorism or cyber warfare. The training is conducted in a simulated environment, which might imitate a massive cyber attack or any other type of incident. This is truly a valuable experience, and Russia has much to learn in this area.

Of the CERTs existing in Russia today, perhaps the most active one is CERT-IB. All other CERTs in fact are not fully operational, or at least are narrowly specialized and work only to solve specific issues, such as detecting and reacting to attacks on scientific institutions. Examples of such CERTs are RU-CERT and the CERT of Web Plus, the largest St. Petersburg-based Internet Service Provider (this CERT serves its own clients as well as those of the provider). We should also mention the Center for Computer Emergency Response in Information and Telecommunications Networks (ITS) of RF Government Organizations (GOV-CERT)—a project of the FSB. Launched in 2012, it has not yet become fully operational. However, with time this center might reach the level of leading global CERTs, which are reacting to cybersecurity threats 24/7, and aim to meet the needs of government agencies and critical infrastructure objects.

Another possible scenario for collaboration would include exchange of data on cyber threats. A lot of frameworks, platforms, and online projects have been developed for this particular purpose in the ASEAN states. One example is the Philippine HoneyNet, which collects information on cyber threats and network attacks, analyzes it, and offers processed statistics. With the aid of these data, specialists could understand the trends afoot, identify the methods that the hackers use, and possibly gather evidence of illegal activity and then use this to mitigate the threat. Meanwhile, it is of interest that major attacks against targets in the Philippines tend to come from the United States or China; the closest partners are thus also the largest sources of threats in cyberspace.

At the same time, one of the key unresolved problems is the misguided attempts to attribute responsibility for an attack to a country from whose territory it originated. In reality, a specific device or host from which the attack is conducted may be controlled regardless of its physical location by any government or person who happens to be the citizen of another state. If the attack comes from the territory of China or the United States, this does not automatically mean that these countries are behind it. In contrast to threats in the offline world, in cyberspace it is extremely difficult to trace the source. Herein lies the problem of attribution—one of the key challenges that is still not solved and requires international cooperation and joint development initiatives to cope with it.

Concerning the exchange of information, different ASEAN countries are solving this problem in different ways, but a number of common points still can be identified. The first is the presence of a single coordinating body, which, unfortunately, Russia does not yet have, since the various aspects related to information security are at the moment covered by a number of regulating bodies: the vFederal Service for Technical and Export Control, the Federal Security Service, the General Staff of the Russian Armed Forces, Ministry of Internal Affairs, the Central Bank, Ministry of Emergencies, Ministry of Energy, etc. In December 2013, the question came to the agenda on which governmental agency should be responsible for preventing cyber threats during the 2014 Winter Olympics in Sochi. As a result, none of the federal agencies’ representatives was able to confirm that his structure was in charge of the issue. This lack of effective coordination in the highly dynamic environment in which cyber attacks are carried out has an adverse effect on the process of preventing, combating, and minimization of their consequences. The price of a delayed response—a delay even of

84 COMMON AGENDA FOR RUSSIA AND ASEAN IN CYBERSPACE
several minutes, or tens of minutes—would be critical in the field of cyber security. Disabling the system of a critical infrastructure object such as an airport or a dam for a few minutes would lead to catastrophic consequences, which should not be forgotten.

Just to compare: in 2012, at a Cybersecurity Forum in Malaysia, there was discussion of a mechanism for collaboration between various parties. The proposed format was designed to be used both nationwide and internationally, within the ASEAN region and beyond. In the case of Malaysia, the Philippines, and other ASEAN states, private businesses are very actively involved in resolving these issues. In Russia, the links between the private sector and the state in the field of cyber security and exchange of information are not yet as strong as one would want. Certain private initiatives are afoot, but one cannot say that in today’s Russia there is a working, polished process, clear and open to all potential participants.

Currently, per the Presidential Decree of January 15, 2013 (No. 31) “On the development of a statewide system for the detection, prevention and response to cyber attacks against information resources of the Russian Federation” the development of an integrated nationwide system of monitoring and exchange of information on incidents and attacks against governmental ICT assets is underway.

One more important activity is sharing best practices through educational and training programs, and here Russia has some ideas to promote to its ASEAN partners, and vice versa. For example, AP-CERT holds five-day training programs stratified in terms of level and content, offering both the theoretical and practical knowledge necessary to respond to cyber attacks and threats in cyberspace. In recent years, significant numbers of experts from various Southeast Asia states and other regions attended these training sessions. Both Russia and its partners gained experience, which should be actively shared and taken into account. That would help to prevent the situation when certain approaches are elaborated from scratch while existing experience and best practices remain ignored.

**KALININ:** I would like to support what Alexey said on the importance of CERTs in the collaboration between Russia and the Southeast Asia region. In Group-IB I am responsible for our CERT: CERT-GIB, and it is actually the first private CERT in Russia. Group-IB has three offices around the world. In addition to our headquarters in Moscow, we have employees in New York and Singapore, something necessary first and foremost to ensure a 24/7 operating cycle. In 2012 we began to actively engage in regional and specialized global organizations and cooperation formats, such as the Trusted Introducer service, which brings together European teams to respond to cyber incidents, and the Global Forum of groups for Incident Response and Security (FIRST).

All these formats enable collaboration of local CERTs worldwide, and each of these networks has accredited many dozens of national and private teams already. We are also developing a dialogue on cooperation with AP-CERT. Group-IB applied for membership in 2013, and should become a member before the end of 2014, as soon as AP-CERT moves to a new document-processing standard. The adoption of CERT-GIB to AP-CERT sets a precedent for Russian organizations. Taking into account the skills and experience of AP-CERT in terms of training programs, as well as their influence in the ASEAN region, we very much look forward to this, and plan to actively exchange knowledge with our partners in the Southeast Asia.

So, what are the key advantages and strengths of our own CERT in Russia? We have a special domain-name-blocking function in top-level domains .RU and .РФ. We may block the delegation of domain names in these domains, if the resources using the domain name are used for spreading malware, or establishing and operating botnet controllers and phishing software. Such a practice of delegation of certain competences in this area to private entities is quite rare worldwide. The Thai Incident Response Center (ThaiCERT) demonstrated high interest in our experience at the FIRST conference in Bangkok in the summer of 2013, and we have witnessed such from many different organizations. We were delegated serious authority, yet, at the same time, our domain-related activities are verified by the domain names Registrar, and in the two years during which we have conducted such activities, no conflicts with regard of legality of this scheme took place. The competences I mentioned were delegated to Group-IB by the Coordination Center of the top-level domains .RU and .РФ.

In March 2013, Group-IB became one of the participants in the International Multilateral Partnership against Cyber Threats (IMPACT) mechanism. Since 2011 IMPACT has been operating as an international PPP with the International Telecommunication Union (ITU).
Participation in this partnership proved quite useful for us in terms of interaction with the ASEAN region. Previously, when we detected and recorded attempted attacks targeted at Russian citizens or entities from the territory of the ASEAN countries, it was not easy to find a point of contact with the relevant government authorities in the region. The source of the problem was not just the language barrier, but also a lack of motivation to interact; some of our requests were also ignored for whatever other reason. Now, when there are institutional partners or companies present in the region—in particular, our partners in IMPACT—the dynamics of collaboration has rapidly increased. After we joined IMPACT and AP-CERT we saw a significant upsurge in the number of constructive responses from foreign partners, including from ASEAN countries.

Interaction and the exchange of information are a mutual endeavor. Apart from receiving specific data from specialized bodies in the ASEAN countries, after joining IMPACT we also started to receive a lot of data about Russian resources that ASEAN countries, for their part, would like to block. We also exchange information with the Russian authorities, as well as business entities and CERTs, including Kaspersky Lab and a variety of organizations in other countries. And of course we share certain information in the FIRST framework. In 2014 we planned to have data exchange with the Spanish CERT, and there were also negotiations on collaboration with the CERT in Germany. As soon as Group-IB joins AP-CERT, we will immediately start talks with the Chinese CERT. Collaboration with our Chinese colleagues is of great interest, since many attacks—including those against Russian targets—go through Chinese territory. We are always ready to cooperate in terms of regulatory documents, something that periodically occurs in addition to the exchange of data on attacks and incidents.

VASILIEV: Concerning the activities of CERT-GBI, I would like to remind you that this is state in charge of providing security to society and individuals in Russia, and, in the case of computer attacks, nothing prevents legal entities from requesting assistance from the law enforcement agencies. It is unclear why this is not done in some cases, and why there is such a trend to seek assistance and incident investigation from some non-governmental structures. In Russia, there is a network of national contact points operating 24/7 as part of the Roma-Lyon Group of the former G9. The Russian National Contact Point is Department “K” of the Ministry of Interior, whose employees actively participate in the exchange of information and respond to requests concerning computer incidents and Internet attacks. After being received, requests are processed and a prompt response is generated. Over 60 countries are part of the network; back in 2013, cooperation on this track was quite active.

One of the problems, in my opinion, is that within the established formats of collaboration we do not always receive enough information. In 2013, the Russian Ministry of Interior conducted an operation codenamed Sornjak (Weed). The purpose was to identify web resources disseminating child pornography on the Internet. As a result, over a thousand such websites were identified, many of which were registered and hosted outside of Russia. A large number of requests were sent to the states in whose jurisdiction the related sources were registered, with the overwhelming majority of requests—over 800—sent to the United States. Unfortunately, we received only four responses to all these requests; this proves that the efficiency of transborder cooperation in some aspects remains unacceptably low. We believe that there is a lot of work to be done and improvements to be made in this area.

MEDRISH: CERTs are a key point for many issues, so they should be discussed. Certain Russian entities, for instance the RU-CERT, are in essence not CERTs, since they do not perform the functions of incident response in computer networks. A full-fledged CERT works like a fire brigade: i.e. a group of people who normally may work in different places, yet when a cyber incident breaks out, they gather in one place as quickly as possible and begin to resolve the problem at hand. To be capable of this, the members of the CERT should be regularly and intensively trained—something that has been very correctly pointed out by Alexey Lukatsky. In addition, they must possess a working toolkit for responding to cybersecurity incidents effectively. Given these requirements and criteria, only Web Plus, which calls its team a CERT, may, with a certain stretch, actually be regarded as such. I will not speak as to the situation in the Russian security services; in fact, they could establish CERT that meets global practices and criteria, and operates accordingly.

Unfortunately, Russia lags behind the world’s best practices in terms of the development of CERTs. At the legislative level of legislation, we lack a structure of a CERTs network with a
CERT Coordination Center (CERT/CC) at the top, serving as a hub and contact link to the activities of other teams. At the same time, global experience shows that CERTs can work efficiently regardless of their formal status, be they government agencies, private companies, or noncommercial organizations. As an example, we might mention the United States, where there is a CERT Coordination Center at Carnegie Mellon University, which in one way or another coordinates the activities of civilian CERTs. Separate CERTs exist only as part of the military. In total, the United States has some 50–60 CERTs, and at some private companies, such as Adobe Systems and other large transnational corporations, where completely different types of activity necessitating a variety of IT processes take place, there are two CERTs or more within the corporate structure.

Thus the interaction of CERTs from different countries in the framework of a CERT/CC carries the potential for the exchange of experience and best practices between Russia and the countries of Southeast Asia. The Internet cannot be confined to the borders of any state so we should look to the example of AP-CERT, which has been resolving issues that concern the entire region through cooperation between multiple governments. The ASEAN countries have learned to do this quite successfully.

I would like to encourage the people involved in the process of making decisions in Russia to see that it is imperative to move along this path, which could lead to the establishment of a flexible and efficient CERT system, repulsing cyber-threats in accordance with the world’s best practices. With this appeal, I would like to conclude our discussion.

NOTE

1 This publication makes use of materials from the joint Roundtable of PIR Center and the ASEAN Center at MGIMO, entitled “Common Agenda for Russia and ASEAN in Cyberspace: Countering Global Threats, Strengthening Cybersecurity and Fostering Cooperation” held in Moscow on December 10, 2013.
Evgeny Buzhinsky

DOES THE INF TREATY HAVE A FUTURE?

The question of whether Russia should withdraw from the 1987 Intermediate-Range and Shorter-Range Nuclear Forces Treaty (INF) is increasingly being raised by the expert community. What is more important, several Russian officials have said that the treaty is detrimental to Russian national security.

The main proponent of a Russian pullout from the treaty is Sergei Ivanov, the Head of the Russian Presidential Staff. The first time he raised that issue was in October 2003, when he served as Minister of Defense, during a meeting with his U.S. counterpart Donald Rumsfeld in Colorado Springs. Rumsfeld, who is known for his opposition to any arms control agreements, responded quite cautiously to Ivanov’s proposal. He said, in effect, that Russia was free to pull out of the INF if it chose to, and that Washington would have no objections. Shortly before that, the Americans unilaterally withdrew from the 1972 Anti-Ballistic Missile Treaty (ABM Treaty), drawing almost unanimous condemnation from the international community. They were clearly not in a good position to initiate the collapse of yet another disarmament treaty, which is an important element of maintaining strategic stability.

Another important consideration is that, unlike the ABM Treaty, the INF Treaty in fact does not hamper Washington’s defense plans in any way. However, to explain and develop these findings I would like first to highlight the historic background of the Cold War events that brought to life the idea of the Treaty and to provide a closer look at the negotiations on the document, its adoption, and its implementation.

HISTORICAL BACKGROUND: HOW THE COLD WAR ARMS RACE LED TO THE MISSILE STALEMATE

Nuclear confrontation between the Soviet Union and the United States began in the late 1950s and early 1960s, when the Americans deployed their Thor and Jupiter intermediate-range ballistic nuclear missiles in Turkey, Italy, and Britain. The flight time of American missiles targeted at the Soviet Union was thereby reduced from 30 minutes to only 8–10 minutes. In 1962, the Soviet Union delivered a symmetric response by stationing its R-12 intermediate-range ballistic nuclear missiles in Cuba. Moscow rightly believed that deploying such missiles in Europe would not be an adequate response. The flight time of Soviet nuclear missiles stationed in Cuba was exactly the same as the flight time of U.S. missiles stationed in Europe.

Washington refused to accept such parity, and initiated the Cuban missile crisis, which was settled by the pullout of Soviet missiles from Cuba and the U.S. missiles from Europe. In the wake of that crisis, the United States abandoned its plans to deploy intermediate-range ballistic nuclear missiles in Europe for almost two decades. In 1979, however, NATO took the decision to station intermediate-range nuclear missiles in Western European countries while at the same time launching negotiations with Moscow on nuclear and conventional arms reductions. The United States hoped that the Soviet Union would not respond by deploying its missiles in Cuba, so as to avoid a repetition of the 1962 crisis—and that even if Moscow
tried to do so, it would fail because the United States had already established a naval blockade of Cuba by that time.

The plan was to deploy 108 Pershing-2 intermediate-range ballistic missiles and 464 BGM-109G land-based cruise missiles in Europe. The decision was explained by the need to eliminate the imbalance resulting from the Soviet deployment of the new Pioneer intermediate-range ballistic missiles with MIRVed warheads, which replaced the obsolete R-12 and R-14 intermediate-range missiles. At the time, NATO had almost twice the Russian number of intermediate-range nuclear weapons delivery systems (missiles and bombers, including carrier-based aircraft). To be more precise, NATO had 1,800 such systems, and Russia 1,000.

The situation clearly was not turning in the Soviet Union’s favor because its Pioneer missiles posed no direct threat to U.S. territory, whereas Washington’s Pershing ballistic missiles and cruise missiles posed a direct threat to vital military facilities on Soviet territory.

During the period from 1980 to 1983 the Soviet Union put forward a number of proposals on reductions of intermediate-range nuclear weapons stationed in Europe. Under the latest of those proposals, the Soviet Union and NATO were to achieve parity in terms of intermediate-range nuclear bombers. The Soviet Union was also prepared to eliminate all but 140 of its Pioneer intermediate-range ballistic missiles. In other words, it agreed to keep fewer of such missiles than France and the UK had in their arsenals at the time. The United States, meanwhile, was asked to abandon plans for deploying its intermediate-range ballistic missiles and land-based cruise missiles in Europe.

In 1981 the Americans made their own counterproposal. Under the so-called zero option, they agreed not to deploy Pershing-2 and cruise missiles in Western Europe in return for the elimination of all Soviet intermediate-range missiles stationed in both the European and the Asian parts of the country. In essence, Washington wanted Moscow to eliminate the 600 intermediate-range ballistic nuclear missiles it had already deployed, in return for the United States undertaking not to deploy in Western Europe its missiles that were still being developed at the time. After that the Americans made several other proposals aimed at achieving numerical parity between the Soviet Union and NATO in intermediate-range missiles. All of these proposals, however, were rejected by the Soviet leadership because none of them contained an obligation by Washington not to deploy U.S. missiles in Europe. In late 1983 the United States began to deploy its intermediate-range missiles on the European continent.

The Soviet Union considered several possible responses, from increasing the numbers of intermediate-range ballistic missiles stationed in Eastern Europe to deploying Pioneer missiles in the Chukotka region close to Alaska.

THE INF TREATY: SIGNING AND IMPLEMENTATION

The Soviet approach to the problem of American intermediate-range missiles in Europe changed radically following the arrival in 1985 of the new Soviet leader, Mikhail Gorbachev. To begin with, Moscow unilaterally suspended the deployment of its own missiles and other response measures in Europe. Then in the spring of 1987 Gorbachev proposed the so-called double global zero plan. The proposal included the elimination of all U.S. and Soviet intermediate-range (1,000–5,500 km) missiles, as well as all shorter-range (500–1,000 km) missiles (see Table 1). The plan was accepted and formalized in the 1987 INF Treaty, signed for an indefinite term.

STRIKING THE BALANCE: QUANTITATIVE EFFECTS ON THE INF TREATY FOR THE PARTIES’ ARSENALS

To achieve compliance with the INF Treaty, the Soviet Union had to eliminate more than twice as many missiles as the United States (1,836 vs. 859), and almost three times as many launchers (851 to 283). The Soviet missiles eliminated under the treaty were capable of carrying four times as many nuclear warheads as the American ones (3,154 vs. 846).

The only type of missile which the United States eliminated more of than the Soviet Union was land-based cruise missiles (443 vs. 80). That, however, was not a major concession by the
Table 1. Soviet and U.S. intermediate-range and shorter-range missiles and launchers eliminated under the INF Treaty

1. Deployed missiles
2. Non-deployed missiles
3. Deployed and non-deployed missiles in total
4. Deployed launchers
5. Non-deployed launchers
6. Deployed and non-deployed launchers in total

1. **Soviet Union**

<table>
<thead>
<tr>
<th>INTERMEDIATE-RANGE MISSILES</th>
<th>SHORTER-RANGE MISSILES</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSD-10 R-12 R-14 RK-55</td>
<td>TOTAL OTR-22 OTR-22 TOTAL</td>
</tr>
<tr>
<td>1  405  65  -  -</td>
<td>470  220  167  387</td>
</tr>
<tr>
<td>2  245  105  6  84</td>
<td>440  506  33  539</td>
</tr>
<tr>
<td>3  650  170  6  84</td>
<td>910  726  200  926</td>
</tr>
<tr>
<td>4  405  79  -  -</td>
<td>484  115  82  197</td>
</tr>
<tr>
<td>5  118  6  -  6</td>
<td>130  20  20  40</td>
</tr>
<tr>
<td>6  523  85  -  6</td>
<td>614  135  102  237</td>
</tr>
</tbody>
</table>

2. **United States**

<table>
<thead>
<tr>
<th>INTERMEDIATE-RANGE MISSILES</th>
<th>SHORTER-RANGE MISSILES</th>
</tr>
</thead>
<tbody>
<tr>
<td>PERSHING-2 BGM-109G TOTAL</td>
<td>PERSHING-1A PERSHING-1B TOTAL</td>
</tr>
<tr>
<td>1  120  309  429</td>
<td>-  -  170</td>
</tr>
<tr>
<td>2  127  133  260</td>
<td>170  -  170</td>
</tr>
<tr>
<td>3  247  442  689</td>
<td>170  -  170</td>
</tr>
<tr>
<td>4  105  109  214</td>
<td>-  -  -</td>
</tr>
<tr>
<td>5  51  17  68</td>
<td>1  -  1</td>
</tr>
<tr>
<td>6  156  126  282</td>
<td>1  -  1</td>
</tr>
</tbody>
</table>

United States because Washington also had large numbers of sea-based cruise missiles (Tomahawk) and air-based cruise missiles (ALCM-B). The total number of those missiles was expected to reach 7,000 by the mid-1990s. The magnitude of unilateral concessions made by the Soviet Union during the INF talks is best demonstrated by the Soviet leadership’s decision to destroy all 239 of its latest Oka ballistic missiles, which had a range of 400km.

**FROM PAST TO PRESENT: THE INTERMEDIATE RANGE MISSILES ISSUE ON TODAY’S VOLATILE INTERNATIONAL AGENDA**

Speaking at a meeting with leading national security experts in the Russian town of Sarov (previously Arzamas-16, the Soviet center of nuclear research) on February 2012, Vladimir Putin, who was serving as prime minister at the time, made his first remarks about the INF Treaty. What he had said on the subject deserves to be quoted verbatim with regard to the subject of this article:

"Other countries are energetically improving their intermediate-range missiles, and almost all our neighbors are developing these weapons systems. The Soviet Union and, obviously, the Russian Federation have relinquished intermediate-range missiles by signing a treaty to that effect with the United States. This is not entirely reasonable because the Americans don’t have any real need for such systems. There is nowhere they can put them to any real use. On the other hand, for the Soviet Union, and..."
especially for Russia in its current situation, considering that our neighbors are developing these offensive systems, such a decision was controversial, to say the least.  

This message was later echoed in the statements of other Russian officials and decision-makers in the field of strategic security. In 2013 Sergey Ivanov spoke once again to the effect that the ban on intermediate-range missiles cannot remain in place indefinitely. He reiterated the idea voiced by Vladimir Putin in Sarov that the United States had never had any real need for such missiles—and in the final analysis, he was quite right.

To a certain extent, the U.S. position with regard to intermediate-range ballistic missiles and land-based cruise missiles is similar to its position with regard to non-strategic nuclear weapons. Washington requires neither class of weapons to protect its national territory. It can use them only as forward-based weapons. Now that the Cold War is over, the Western European NATO members hardly require such weapons on their territory.

What, then, is the real situation with intermediate-range missiles at this time? The situation has changed very radically since the INF Treaty was signed.

First, six countries (China, India, Pakistan, Israel, Iran, and North Korea) have land-based intermediate-range ballistic missiles that can carry nuclear warheads. Furthermore, several other countries have missiles of this class armed with conventional warheads. At the same time, Russia's attempts to make the INF Treaty multilateral, which were undertaken in the mid-2000, have found little support in the international arena, which was only to be expected.

Having this in mind, it may be assumed that Russia has two main options for compensating the loss of the land-based intermediate-range missile capability. The first is to improve and strengthen its strategic nuclear arsenal, while the other implies deployment of sea-based and/or air-based intermediate-range missiles.

As already mentioned, the option of withdrawal from the INF Treaty is being studied, but for the foreseeable future such a solution is unlikely to appear. A unilateral Russian pullout would cause political complications, and there is little hope of the United States agreeing to rescind the treaty by mutual consent. In fact, the treaty has moved up Washington's agenda in recent months over allegations that Russia is developing a new land-based cruise missile, the R-500.

THE INF TREATY ISSUE FROM THE U.S. TODAY'S PERSPECTIVE: THE GAME OF WITHDRAWAL NOT WORTH THE TROUBLE?

In July of 2014 U.S. President Barack Obama wrote a letter to his Russian counterpart Vladimir Putin, where he expressed concern about the GLCM R-500 tested at a range of 400km, as well as the R-26 ICBM Rubezh, which, according to American data, was run at a distance of less than 5500km. In fact, the R-26 was tested at a range of 6500km and, in accordance with the provisions of the START Treaty, is considered an intercontinental ballistic missile. The emergence of such a letter can only be seen in the context of the general tensions between Russia and the United States against the background of the Ukrainian crisis, because, unlike Russia, the Americans do actually violate the provisions of the INF Treaty, at least in two respects:

- the use of two stages of ICBMs to be disposed of as targets simulating medium-range ballistic missiles to test interceptor missiles;
- mass production and use of unmanned combat aerial vehicles (UCAV) MQ-1 Predator and MQ-9 Reaper.

In addition, the United States is testing the new generation of UCAV (X-47), which can also be interpreted as a direct violation of the INF Treaty. In fact, all long-range UCAVs, strictly speaking, fall under the contractual definition of "cruise missile" (paragraph 2 of Article II of the INF Treaty), of which development is prohibited in accordance with the Treaty. Remembering these sins, the United States for many years avoided discussions on violations of the INF Treaty.

The Americans realize that resuming the development and manufacture of new land-based intermediate-range ballistic missiles does not make much sense militarily, especially in view
of the financial burden such a move would impose on the country’s shrinking defense budget. As already explained, such missiles are a forward-based weapon, and there is little confidence that Washington’s allies in Europe and Asia (including Japan and South Korea) would allow such weapons to be deployed on their territory now that the Cold War is over, with Russia posing no real threat to their national security.

***

Taking all the aforesaid into consideration, I am confident that the INF Treaty will remain in force for the foreseeable future, barring some radical shifts in the area of global geopolitical stability. Such shifts appear extremely unlikely at this moment.

NOTES

1 “War and Peace: Terms and Definitions,” Military-Political Dictionary under the general editorship of Dmitry Rogozin, Moscow, 2011.

The practice of adopting State Armament Programs as overarching policy documents that set out weapons development and procurement targets was established fairly recently in Russia. The SAP-2020 program, approved in 2011, is the fourth such program in post-Soviet Russian history. The existence of these programs points to the Russian government’s aspiration to develop a long-term and systemic approach in this area. But their actual implementation has not exactly been an unqualified success so far. In fact, most of the targets set out in the three previous SAP programs were not met.

What, then, is the current state of the SAP-2020 program, which is far more ambitious than all of its predecessors? The program includes a rapid increase in defense spending, suggesting that the government now regards the rearmament of the Armed Forces and technological upgrade of the Russian defense industry as a much more important priority. But how realistic are the SAP-2020 targets and plans? Having emerged from a long period of decline, can the Russian defense industry actually deliver such a large increase in defense R&D and manufacturing? How much progress has already been made on individual SAP targets? And what are the risks of those targets not being met once again?

In fall 2012 Deputy Prime Minister Dmitry Rogozin said that the Commission for the Defense Industry was working on a new armaments program for the 2016–2025 period. The plan is to submit the program for the president’s approval in July 2015. Russian officials claim that the implementation of the current SAP-2020 program will continue, and that the second half of SAP-2020 will merely overlap with the first half of the new program. In particular, under the MoD plans approved in July 2013, the rearmament projects in the Army and the Navy will continue in accordance with the SAP-2020 targets.

**KEY SAP-2020 TARGETS**

The main objective of the SAP-2020 program is to increase the proportion of new weapons and hardware in service with the Russian armed forces to 70 percent by 2020. That part of the program will cost 20.7 trillion roubles, including 19 trillion to be spent on Army, Air Force, and Navy rearmament. New weaponry and hardware contracts will account for about 70 percent of that figure; repair and upgrade of the existing weaponry will take up 15 percent; and weapons R&D programs another 15 percent. A further 3 trillion roubles will be spent on technology upgrade across the Russian defense industry. Publicly available figures regarding the financing of individual components of the SAP-2020 program, as well as reports concerning specific projects to be undertaken as part of that program, are incomplete and keep changing every now and then. Nevertheless, the general outlines of the program appear to be as follows (see Table 1).

The targets outlined above are very ambitious—but the actual implementation of the program has already run into trouble. One of the worrying signs is that in June 2013 the Ministry of Finance and the MoD agreed to defer some of the SAP-2020 spending originally slated for 2014–2016 to the 2017–2018 period. As a result, some of the new weapons procurement
### Table 1. Approximate Targets and Key Objectives of the SAP-2020 Program

<table>
<thead>
<tr>
<th>Title</th>
<th>Price, trillion roubles</th>
<th>Share in total, %</th>
<th>Procurement and/or R&amp;D plans</th>
</tr>
</thead>
<tbody>
<tr>
<td>Army and Airborne Troops</td>
<td>2.6</td>
<td>14</td>
<td>2,300 main battle tanks; 2,000 artillery systems; 10 brigade-size units of Iskander-M tactical ballistic missiles, including 160 twin launchers and 320 missiles; nine brigade-size units of the S-300V4 SAM systems; more than 30,000 vehicles. Deliveries of new tanks, self-propelled artillery and armored combat vehicles are expected to commence in 2015</td>
</tr>
<tr>
<td>Navy (including naval nuclear forces)</td>
<td>4.5–5.0</td>
<td>26</td>
<td>8 Borei-class nuclear missile submarines and 120–130 Bulava SLBMs; eight Yasen-class multirole submarines; eight non-nuclear submarines; 51 ships, including 14–15 frigates and up to 25 corvettes</td>
</tr>
<tr>
<td>Aerospace Defense</td>
<td>3.4–4.0</td>
<td>17</td>
<td>56 batteries of the S-400 SAM system, including 448 launchers and 1,798 guided AA missiles; 38 batteries of the S-500 SAM system, including 300–460 launchers and 1,220–1,820 missiles; an integrated air and space defense command and control system; 4 Voronezh radar stations; and 100 spacecraft. The entry of the S-500 SAM system into service is scheduled for late 2016</td>
</tr>
<tr>
<td>Strategic missile troops</td>
<td>1.0</td>
<td>6</td>
<td>270–280 Yars ICBMs; development of a new solid-fuel ICBM (Project Rubezh, possibly based on the Bulava SLBM design) and of a new liquid-fuel ICBM</td>
</tr>
<tr>
<td>Air Force Others</td>
<td>4.0–5.0</td>
<td>21</td>
<td>600 planes and 1,000–1,100 helicopters New communication, command-and-control, and reconnaissance systems, new infantry soldier kit, etc.</td>
</tr>
<tr>
<td>Others</td>
<td>2.7</td>
<td>14</td>
<td></td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>18–19</strong></td>
<td><strong>100</strong></td>
<td></td>
</tr>
</tbody>
</table>

Source: Nezavisimoe Voennoe Obozrenie (journal), 2013, and other open sources in the Russian media.

Contracts, especially those made under long-term programs, may have to be postponed until the period covered by SAP-2025. There have been reports in the media suggesting that the delays will primarily affect the new Borei-class nuclear missile submarines.

### THE NAVY

It has already become quite obvious that the naval weaponry section of the SAP-2020 is running behind schedule. In May 2013 Dmitry Rogozin admitted that there was an “obvious danger of the targets being missed” with regard to the shipbuilding and ship repair programs. Shortly before he made the statement, the government replaced senior executives at the United Shipbuilding Corporation (OSK), who were accused of “intentionally underestimating the costs” when signing contracts for nuclear submarines.

The target of entering into service seven new Borei-class nuclear missile submarines and eight Yasen-class multirole subs in the 2013–2020 period does not seem realistic, either. To meet this target, the Russian shipyards would have to ramp up their output to levels not seen since the heyday of the Soviet defense industry. To illustrate, a total of 18 nuclear submarines were built in Severodvinsk in the 1980–1988 period, with each sub taking four and a half to five years to complete (see Table 2).
Table 2. Borei and Yasen Submarine Programs

<table>
<thead>
<tr>
<th>Name</th>
<th>Laid down</th>
<th>Launched</th>
<th>Current State</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Borei-class nuclear missile subs</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Alexander Nevsky</td>
<td>03/2004</td>
<td>12/2010</td>
<td>Entered into service in December 2013</td>
</tr>
<tr>
<td>Vladimir Monomakh</td>
<td>03/2006</td>
<td>12/2012</td>
<td>To enter into service on December 19, 2014</td>
</tr>
<tr>
<td>Knyaz Vladimir</td>
<td>07/2012</td>
<td></td>
<td>On the stocks</td>
</tr>
<tr>
<td>Knyaz Oleg</td>
<td>07/2014</td>
<td></td>
<td>On the stocks</td>
</tr>
<tr>
<td>Mikhail Kutuzov</td>
<td></td>
<td></td>
<td>To be laid down in December 2014</td>
</tr>
<tr>
<td><strong>Yasen-class nuclear submarines</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Severodvinsk</td>
<td>1993</td>
<td>2010</td>
<td>Entered into service on June 17, 2014</td>
</tr>
<tr>
<td>Kazan</td>
<td></td>
<td>2009</td>
<td>To be launched in 2015</td>
</tr>
<tr>
<td>Novosibirsk</td>
<td></td>
<td>07/2013</td>
<td>On the stocks</td>
</tr>
<tr>
<td>Contracts have been signed for another three Yasen-class nuclear submarines.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Krasnoyarsk</td>
<td>07/2014</td>
<td></td>
<td>On the stocks</td>
</tr>
</tbody>
</table>

After the decision was made to build the Yury Dolgorukiy, 16 years passed before the submarine entered into service. The Severodvinsk project has been ongoing for about 20 years now, but the sub entered into service only this summer. After the Alexander Nevsky and the Vladimir Monomakh were laid down, it took six years to launch them; only one of them has entered into service so far.

The corvette and frigate programs are not faring much better. The Navy plans to have up to 25 of the Project 20380 and Project 20385 corvettes in service by 2020. Only three Project 20380 ships were in service in 2013, with another three on the way and a contract signed for one more ship. The Project 20385 corvette program has been discontinued because it was deemed too expensive. Only a single Project 20385 ship will probably be built; instead of all the others, the MoD will receive cheaper ships that are still on the drawing board, with no clear deadline for the completion of R&D. As for the Project 22350 and Project 11356 R/M frigates, only a single ship of each type is nearing completion. In other words, meeting the SAP-2020 targets for frigates and corvettes would require another 27-28 ships to be built and entered into service in 2013-2020 in addition to the ships that are already under way or have been delivered to the Navy. That is patently unrealistic.

It is therefore safe to assume that by 2020 the Russian Navy will have no more than four Borei-class nuclear missile submarines; four Yasen-class multirole nuclear submarines; up to eight corvettes; and four or five frigates. That is less than half of the target set out in the SAP-2020 program.

THE AIR FORCE

At first glance, the Air Force component of the SAP-2020 program is looking much better. By mid-2013 contracts had been signed for about 350 combat and transport aircraft, 55 trainers, almost 200 attack helicopters, and 100 transport/attack helicopters (see Table 3).

Meeting the SAP-2020 targets would require the Russian aerospace industry to ramp up its output very significantly. In 2011 that industry delivered 21 planes and 82 helicopters to the Russian Air Force. In 2020 the figures were 42 planes (including 20 combat aircraft) and 57 helicopters. The target for 2013 is about 60 planes and more than 100 helicopters, with another 100 planes to be delivered in 2014. In other words, aircraft production must rise fivefold in 2015 compared with 2011. There are serious doubts about the feasibility of such
Table 3. **Approximate Composition of the Russian Air Force and Air Defense Fleet in 2012 and 2020**

<table>
<thead>
<tr>
<th>Title</th>
<th>2012</th>
<th>Total</th>
<th>Based on contracts signed or ready for signing as of mid-2013</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tactical bombers</td>
<td>343</td>
<td>170–190</td>
<td>New: 124–140 Su-34</td>
</tr>
<tr>
<td>Ground attack aircraft</td>
<td>200</td>
<td>200</td>
<td>Upgraded: 36 Su-25</td>
</tr>
<tr>
<td>Transports</td>
<td>210</td>
<td>352</td>
<td>New: 39 Il-76 MD 90A</td>
</tr>
<tr>
<td>Attack helicopters</td>
<td>374</td>
<td>576</td>
<td>New: 140 Ka-52; 96 Mi-28N; 48 Mi-35N</td>
</tr>
<tr>
<td>Transport/attack helicopters</td>
<td>519</td>
<td>978</td>
<td>New: 100 Ka-60</td>
</tr>
</tbody>
</table>

plans, especially taking into account the ongoing difficulties with the manufacturing of some crucial components.

Russian experts also emphasize that with the exception of the T-50 (PAK FA) multirole fighter, all the other planes being procured under the SAP-2020 are merely upgraded versions of Soviet-era technology. As for the T-50, the first planes are to be delivered to the Air Force in 2015, with a total of 60 aircraft to be supplied by 2020. Experts reckon that this particular target is totally unrealistic.

**AEROSPACE DEFENSE**

A key element of the SAP-2020 aerospace defense procurement is large deliveries of the S-400 and S-500 SAM systems. The first battery of the S-400 (seven launchers with four missiles apiece) entered service in 2007. By late 2012 there were nine operational S-400 batteries, meaning that annual production of the S-400 has averaged 1.5 batteries. In order to meet the target for 2020 (56 batteries), an average of 6.5–7 batteries must be deployed every year, requiring a fourfold increase in their manufacturing. To that end the government has decided to build three new production facilities. Two of them, costing a total of approximately 80 billion roubles, are already being built in Kirov and Nizhniy Novgorod. Experts doubt, however, that Russia has sufficient numbers of qualified specialists to man these new facilities.

Another SAP-2020 target is to equip 38 divisions with the S-500 systems. Little is known about the S-500. According to some reports, it is an upgraded version of the S-400, capable of taking out ballistic targets traveling at up to 7 km/sec. According to the MoD’s plans, mass production of the S-500 should commence no later than 2017, although the first prototype may be ready only in 2013. This makes the system’s entry into service and the beginning of its mass production before 2017 highly unlikely. Besides, the capability of the S-400 and S-500 systems is seriously undermined by the absence of a missile capable of engaging targets at altitudes of over 30km. In the summer of 2012 it was reported that such a missile (known as Product 40N6E, and very similar in terms of performance to the U.S. missiles used in the Patriot-PAC 3 system) had been tested successfully—but there have been no reports since then about that missile entering service or mass production.

**STRATEGIC NUCLEAR FORCES**

Over the two years since the New START treaty entered into force, the Russian strategic nuclear arsenal has shrunk very slightly. But in terms of the key indicators such as the numbers of deployed delivery systems and warheads fitted onto these systems, Russia has already descended below the ceilings mandated by the treaty. Before the end of this decade Russia will have to decommission about 200 of the Topol, SS-19 and SS-18 ICBMs currently
in service, which carry a total of about 1,170 warheads. The service life of those missiles has already been extended beyond the original deadlines several times, so keeping them in service after 2020 is out of the question. As a result, of the ICBMs that were in service in 2012, only 70 silo-based and mobile Topol-M ICBMs (carrying a single warhead each) and 18 Yars missiles (with three warheads apiece) will be left by 2019-2020.

The Russian Navy, meanwhile, will probably have six Delta-IV nuclear missile submarines left in service, carrying a total of 384 warheads. Russia also has 60-65 Tu-160 and Tu-95 long-range bombers with the latest modifications. In other words, of the 1,500 warheads that were deployed in 2012, Russia will have only 450-470 left by 2020. In order to bring its strategic arsenal up to the ceiling allowed under the New START treaty, Russia will have to manufacture and deploy a sufficient number of delivery systems to carry just over 1,100 warheads.

As already discussed, by 2020 the Russian Navy will probably operate a maximum of four Borei-class nuclear missile subs, carrying a total of up to 64 Bulava SLBMs, with up to 190 warheads between them. To bring the number of deployed warheads up to 1,550, Russia will therefore have to enter into service 260–300 Yars ICBMs, and possibly the new Rubezh solid-fuel ICBM as well. A total of 320-380 new missiles (including the Bulava) will have to be delivered to the armed forces in 2013–2020. That is roughly in line with the SAP-2020 target of 400 new ballistic missiles to be made in the 2011–2020 period. The average annual output of the Votkinsk facility, where these missiles are made, will have to be increased to 40-45 missiles, which is an increase of 50–100 percent compared with the late 2000s and early 2010s.

THE ARMY AND AIRBORNE TROOPS

In February 2012 the MoD decided not to buy any more of the current generation of tanks and armor offered by the Russian defense industry. The ministry is now waiting for the launch of mass production of new ground weaponry based on several universal platforms. These include the Armata heavy tracked platform now being developed by Uralvagonzavod; the Bumerang medium wheeled platform; and the Kurganets-25 tracked platform. Weapons systems based on these platforms are expected to enter mass production in 2015 at the latest. Over the following five-year period between 2016 and 2020, the defense industry will be expected to deliver up to 2,000 main battle tanks, 2,000 artillery systems; and thousands of other armored vehicles designed around the new universal platforms.

SHORTCOMINGS OF THE SAP-2020 PROGRAM

Many of the targets set out in the SAP-2020 program are very unlikely to be met. One of the reasons for this is that the SAP-2020 is essentially a combination of numerous individual rearmament programs across the armed forces. These sub-programs are often based on the ambitions of the top brass and the vested interests of various groupings within the defense industry, as opposed to some kind of strategic vision, geopolitical planning, or realistic assessment of Russia’s economic capabilities.

As a result, the deadlines for many weapons programs set out in the SAP-2020 are unrealistic. To illustrate, the program assumes that the S-500, the Armata universal armor platform, and other major weapons systems will take only two or three years to enter mass production once the first prototypes have been built. That is completely out of the realms of possibility.
Also, some of the SAP-2020 targets require production of various weapons systems to be augmented by 100–400 percent or even more in the space of just two or three years. International experience clearly demonstrates that such a massive and rapid increase in the production of high-tech weaponry is not feasible. The situation is compounded by the fact that the fundamental problems facing the Russian defense industry remain unresolved, and cannot be quickly resolved even if government funding of that industry were to rise sharply.

A SYSTEMIC CRISIS IN THE RUSSIAN DEFENSE INDUSTRY

The sorry state of affairs in the Russian defense industry is illustrated by the MoD’s refusal to buy any Russian-made armor, including the BTR-90 APCs and the T-90 MBTs, for the next five years.

The Russian defense industry currently lacks the capability to produce many high-tech materials and components to the required standards of quality. The previous MoD leadership had publicly recognized the existence of a serious gap between Russia and the world leaders in such areas as microelectronics, computers and IT systems, armor materials, optical-electronic systems, and high-precision weaponry components. According to former deputy defense minister Aleksandr Sukhorukov, in 2012 the Russian defense industry produced only about 40 percent of the required range of electronic components. Russian technology in this area is lagging more than a decade behind the world leaders. Russian developers and manufacturers of weaponry and military hardware are therefore becoming increasingly dependent on imports of electronics and other components.

Experts close to the defense industry leadership estimate that Russia remains internationally competitive in no more than 7–10 percent of critical technologies. There is a growing shortage of skilled labor. Up to 75 percent of manufacturing assets have reached obsolescence; only about 1 percent of them are being replaced every year, whereas the minimum requirement is thought to be 8–10 percent. As a result, the quality of Russian weaponry is deteriorating. The costs of eliminating various defects during manufacturing, testing, and operation of Russian military hardware can be as high as 50 percent of the entire cost of the final product; in the leading global economies that figure is below 20 percent.

FINANCIAL PROBLEMS FACING THE SAP-2020 PROGRAM

The Russian defense industry’s inability to meet the SAP-2020 targets also has to do with inadequate price formation mechanisms. The prices agreed in the weapons contracts often fail to take into account the level of inflation and the growing prices of materials, components, and energy. This puts a squeeze on profit margins, leaving the defense industry unable to invest in modernization programs. The deflators incorporated into weapons program budgets do not adequately reflect the level of inflation, or the growing costs of materials and components. As a result, several years down the line these programs often turn out to be underfunded to the tune of 30–50 percent; weapons deliveries to the armed forces suffer accordingly. Another problem is that most of the funds to be spent under the SAP-2020 are to be disbursed during the second half of the program. Even before the government decided to defer some of the SAP-2020 spending originally slated for 2014–2016, only 31 percent of the financing was to be disbursed in 2011–2015, and the remaining 69 percent in 2016–2020.

The 23 trillion roubles the government has allocated for the SAP-2020 program is the sum of annual spending in 2011–2020 at current prices. In 2010 prices, and adjusted for purchasing power parity, the figure in roubles roughly equals 1 trillion dollars. At first glance, that should be enough to modernize the Russian army and defense industry. But in real prices that figure becomes much less impressive. To illustrate, over the 1999–2012 period Russian defense spending rose by a factor of 20 in current prices (see Figure 1). However, according to the Gaydar Institute, the increase in real prices was a mere 60 percent.

If that trend continues, the actual resources allocated for the SAP-2020 program in 2020 will be only 30–35 percent greater than in 2011 and 2012. This mainly has to do with the rapidly growing prices of weapons and military hardware. For example, in 2000 an average mass-produced tank cost 17 million roubles; 10 years later the figure stood at almost 118 million.
Figure 1. Russian Defense Spending

Source: Gaydar Institute of Economic Policy.

Another example is the Yasen-class nuclear submarine. The first sub in the series cost 47bn roubles; the price tag of the second is 112 billion.

It is safe to predict that the targets set out in the SAP-2020 program will be 50 percent fulfilled at the very best.

By the beginning of the next decade Russia’s conventional forces will still be numerically superior to the forces of the leading European countries—but not nearly as well equipped. The Russian strategic nuclear capability will be slightly below that of the United States by most numerical indicators—but it will be sufficient to maintain nuclear parity. In tactical nuclear weapons, Russia will have superiority over the NATO forces in Europe, and over the Chinese and U.S. forces in the Far East. Russia will maintain and possibly even strengthen its overwhelming numerical and technical superiority over the former Soviet republics, including the Baltic States.

NOTES
1 The analysis in the article makes use of data as of 2013. Some tables and figures are updated as of August 2014.
As the "longest sought and hardest fought prize in the history of arms control," the Comprehensive Nuclear-Test-Ban Treaty (CTBT) not only has strong political symbolism, but also influences nuclear disarmament and nonproliferation in several practical ways. First of all, a ban on nuclear test explosions makes it harder for a would-be nuclear proliferator to produce a working and deliverable nuclear warhead. Second, for the possessors of established nuclear weapons, the CTBT places constraints on the modernization of nuclear arsenals and the development of new and more powerful warheads, limiting improvements to the already tested and verified designs. Third, the Treaty represents a significant step for progress towards a world without nuclear weapons. It not only contributes to the predictability of strategic relations on the global level, but is also an integral element of any current and future regional arrangement in a zone free of nuclear weapons.

The entry-into-force formula, however, requires the ratification of the Annex 2 states before the Treaty comes into effect. Of these 44 countries, 36 have ratified the CTBT. Among the remaining eight, five countries—China, Egypt, Iran, Israel, and the United States—signed, but have not ratified the Treaty, while three others—the DPRK, India, and Pakistan—are yet to sign it. All these countries have diverse, often divergent, interests and find themselves in different strategic environments. Nevertheless, U.S. ratification is viewed largely as a game changer, that could put several key pieces of the puzzle, especially the Chinese one, in place.

The US Senate declined to give consent to the CTBT in 1999 and the Treaty still remains on the floor for the consideration.3 The Obama Administration affirmed on many occasions that it will pursue the ratification and initiated an outreach campaign to inform the Senate and the public on the benefits of the CTBT to U.S. national security; however, well into its second term the Obama Administration is yet to undertake concrete steps towards that ratification. At the same, competing foreign policy priorities exacerbated by simultaneous crises around the world and increasingly partisan politics in Washington in the run-up to the start of the presidential race distract attention from the CTBT, which would have to be among the top priorities of the President to move forward on the floor of the Senate. Finally, if brought back onto the Senate's agenda, the CTBT will have to go through a heated ratification debate and face challenges similar to those of the New START. In this context, a second rejection by the U.S. Senate would be detrimental to the future of the CTBT. Yet, the Treaty, its contribution to strategic stability, and its substantial confidence-building and transparency potential are too valuable to be allowed to slowly fade from the international agenda.

Finally, even U.S. ratification does not guarantee that the remaining States, with some exceptions, will follow suit right away. Diligent work will still be required to secure the outstanding ratifications. Thus, a range of measures within the CTBT framework and within the broader context of a no-testing norm could be explored to maintain political momentum around the Treaty and to inform and facilitate the ratification process in the United States. These measures will have an impact beyond the ratification debate in the United States, by
building trust among the nuclear-weapon states (NWS), as well as improving transparency and thus diminishing negative perceptions among the non-nuclear-weapon states (NNWS) towards the implementation of the disarmament obligations by the NWS.

Russia, China, and the United States, among the NWS, can play a special role in advancing the CTBT. Nuclear weapons are an inseparable element of the strategic relations equation between these states and all three should be interested in maintaining and enhancing their predictability. Additionally, among the official NWS, only Russia, China, and the United States have nuclear test sites and could possibly revert to nuclear test explosions should a political decision be made. This paper explores possible transparency and confidence-building measures from the point of view of Russia, China, and the United States, argues that all three states have something to bring to the table based on the assumption that a return to nuclear testing would upset strategic stability and thus would be detrimental to the national security of all.

RATIFICATION DEBATE IN THE UNITED STATES: ROLE OF RUSSIA AND CHINA

Even though President Obama in his Prague speech in April 2009 promised to pursue the ratification of the CTBT “immediately and aggressively” and pledged in June 2013 in Berlin to “build support in the United States to ratify” the CTBT, the difficulties the White House encountered when pursuing the ratification of the New START suggests that the US ratification of the CTBT is far from certain. At the same time, the fact that 13 Republican Senators supported New START gives hope that if the CTBT is put to the vote again, not only Democrats would support it.

Domestic debate in the United States focuses not only on that country’s ability to maintain a safe, secure, and effective nuclear arsenal in the absence of nuclear testing, but also on potential violations of the Treaty by other countries. The U.S. policy-makers seem to be divided on these issues. For instance, the recommendations on the CTBT were the only item that split consensus on the Final Report of the Congressional Commission on the Strategic Posture of the United States in 2009. While the debate is largely political, the opponents of the Treaty can seize upon any technical ambiguity with the Treaty and its verification regime to derail the ratification drive.

The same report asserted that Russia, and possibly China, continue clandestine hydro-nuclear experiments in violation of zero-yield requirement of the CTBT. In a report by the National Institute of Public Policy (NIPP) published in 2011, the staunchest opponents of the CTBT on the U.S. political scene speculated further by suggesting that Russia may be conducting low-yield nuclear test explosions in Kolba containers designed specifically to neutralize any seismic signals. They further found Russian and Chinese duplicity in the fact that their respective closest International Monitoring Station facilities to the Novaya Zemlya and Lop Nor Nuclear Test Sites are located respectively 1,112 and 783km away, while the United States hosts a seismic station (Mina, NV) less than 200km from Nevada Test Site. The sections below explore how Russia and China could contribute to the ratification debate in the United States and help the Treaty proponents secure the required two-thirds majority in the Senate. Though some believe that the U.S. ratification debate will not be influenced by Russian and Chinese actions, such steps could nonetheless remove potential arguments and obstacles hindering a successful push for ratification.

ENHANCING TRANSPARENCY THROUGH THE INTERNATIONAL MONITORING SYSTEM

The International Monitoring System (IMS) is an unprecedented network of 337—seismic, hydroacoustic, infrasound, and radionuclide—facilities, including radionuclide laboratories, located in more than 90 countries around the world and carefully devised to provide global coverage. The data from the stations are available to all CTBT signatories in near-live time format. Upon the entry into force of the CTBT, the IMS should serve as the basis for the detection of possible violations of the Treaty.

As far as the verification regime is concerned, the NIPP argument on the location of the IMS stations on Russian territory does not withstand sound scientific analysis. Because of the geological structure of the Novaya Zemlya Test Site the threshold of the detection of seismic

104
events is very low and does not require the location of the IMS seismic stations to be in close proximity. In fact, the Norwegian Seismic Arrays (NORSAR)—in particular, the two arrays on Spitsbergen and in northern Norway—operated jointly with the United States are uniquely prepared to detect minor seismic events of Richter magnitude 2.0, "which corresponds to a fully coupled nuclear explosion of about 0.01 kilotons TNT (i.e. 10 tons TNT)."

The United States, Russia, and China host the largest segments of the IMS on their territory: 42, 36, and 14 facilities respectively. It reflects the responsibility of the NWS to host and maintain a significant portion of the CTBT verification regime and constitutes a substantial transparency measure as the data from these stations are accessible to all CTBT States Signatories regardless of their size, influence, and financial contribution. It is the requirement of the Treaty that by the time of its entry into force, the IMS should be fully functional and the Provisional Technical Secretariat of the Preparatory Commission for the Comprehensive Nuclear-Test-Ban Treaty Organization (CTBTO) is tasked with the build-up of the verification network.

The completion of the U.S. segment of the IMS corresponds to the completeness of the IMS on the whole and stands at about 90 percent. However, Russia and China are below this number. In 2011, several Russian high-ranking diplomatic and military officials "expressed [Russia's] aspiration to complete the build-up of IMS facilities on its territory by 2012," becoming the first among the P5 countries to do so. Since then, however, the timelines according to Deputy Defense Minister Anatoly Antonov shifted to the end of 2014/beginning of 2015. Progress on IMS completion in Russia and other NWS specifically highlights the Chinese contribution to the verification regime.

As a responsible country, China has a lot to contribute to the IMS, as well as to benefit from. While the continuous supply of data from the national segment of the IMS is required only upon entry into force of the CTBT, most member-states have certified their IMS facilities and provide data to the CTBTO International Data Center Division. Until recently, China has not been providing data from its stations consistently. However, following the visit of the CTBTO's Executive Secretary Dr. Lassina Zerbo to Beijing in August 2013, China pledged to start providing data to the CTBTO and since January 2014 the data have been flowing to the IDC. It is important that as the part of the testing and evaluation process the data flow continues and leads towards certification (formal acceptance) of the monitoring stations in China. With nine facilities being tested and two others listed as operational in China, the speediest certification of these assets and their addition to the IMS will send a positive signal to CTBT supporters in the United States and worldwide.

As mentioned above, construction of the IMS segments on the territory of the NWS is viewed as a major transparency measure and responsibility under the CTBT. China has long been reluctant to engage in broader transparency measures regarding its nuclear forces, explaining this by the need to make its forces more survivable against a potential first strike. In this context, it views ambiguity as a strategic asset. However, certification of the IMS stations and provision of the IMS data is cost-free as it does not compromise any information on China's nuclear forces. On the contrary, opening up in this regard will enhance China's image and will help to fend off criticism regarding the lack of transparency from both NWS and NNWS alike.

The transparency argument can be taken even further. As far as the CTBT and its influence on strategic relations is concerned, providing information on past nuclear test explosions is another measure that could be conducive to establishing a climate of trust. In the years after the end of the Cold War, Russia and the United States, as well as France and the U.K., provided detailed information on their nuclear testing programs prior to CTBT negotiations, releasing data on the numbers, yield, and purposes of the tests. These data have allowed correcting publicly available estimates even in terms of numbers of the tests. China, which has conducted at least 45 nuclear test explosions, could also provide such information. Releasing information on past activities is a relatively unproblematic approach, involving limited risks, but one that can contribute to the development of a culture of transparency.

Several scholars, however, have suggested that the diplomatic and military communities and members of the Standing Committee of the Politburo of the Chinese Communist Party may find themselves favoring different approaches on the ways to engage the United States on
strategic issues. While this debate has wider implications for strategic relations between China and the United States, it is reasonable to assume that the present Chinese position on the CTBT is heavily influenced by the current stalemate.

**REAFFIRMING THE SCOPE OF THE CTBT**

CTBT opponents in the United States speculate that Russia and China may be involved in clandestine very-low-yield nuclear test explosions. Such concerns could be used to prevent ratification. However, there are several ways to address them.

First of all, during the ratification hearings in the Russian State Duma in 2000, Yuri Kapralov, Director of the Department for Security and Disarmament Affairs of the Russian Foreign Ministry, stated that “qualitative modernization of nuclear weapons is only possible through full-scale and hydronuclear tests with the emission of fissile energy, the carrying out of which directly contradicts the CTBT.” One year earlier, during the hearing in the U.S. Senate, the head of the U.S. delegation at the CTBT negotiations, Ambassador Stephen Ledogar, gave an assurance that Russia agreed on the scope of the CTBT. The Russian press reported the Russian Minister of Defense Sergei Ivanov stating, during his visit to Novaya Zemlya in July 2006, “Russia does not violate its international obligations on the non-conducting of nuclear testing.” While mid-level Russian officials since then have repeated similar assurances, it seems that a high-level political statement specifically targeted at international audiences would be beneficial to assuage the concerns of the skeptics. From the Russian perspective, however, issuing a unilateral statement would not be acceptable: Russia has subscribed to the Treaty, ratified it, and no additional assurances are needed. A joint P-5 statement, which, inter alia, would declare that the NWS reaffirm the scope of the Treaty, may be a more conducive approach. It will not only cover Russia, but will also provide reassurance on behalf of China.

**NUCLEAR TEST SITE AND FACILITIES TRANSPARENCY**

The issue of zero-yield testing, however, goes beyond political assurances and additional measures, such as transparency at nuclear test sites and/or nuclear weapons facilities, could generate a positive impact and enhance trust between the countries concerned.

During the negotiations, the difficulties of verifying low thresholds were well understood. Solutions were not seen as obvious. This situation led to the conclusion of the CTBT without any threshold. For the negotiators, it was clear that 100 percent detection remained impossible and the unofficial threshold for the IMS to detect a 1 KT (or 1000 tons of TNT) explosion under any conditions was suggested as the level defined for catching military-significant testing. At that time no solution was found, but because of the Russian military view that possible violations would be happening at the nuclear test sites, the aforementioned seismic station in Mina, NV was added to the IMS to ensure that the Nevada Test Site would be covered by the CTBT seismic network.

Other proposals circulated as well. For instance, Russia suggested negotiating an agreement outside of the CTBT that would allow placement of additional detectors at the test sites and exchange of information on the experiments conducted. This proposal went along the lines of the 1988 Joint Verification Experiment when, in the process of negotiating a verification protocol to the 1974 U.S.-Soviet Threshold Test-Ban Treaty, teams of scientists from the two countries placed measuring equipment in the shafts before testing at their respective test sites in Nevada and Semipalatinsk. Several experts also suggested a range of measures to verify that the nuclear experiments did not violate the CTBT. Additionally, Russia was interested in test site transparency measures with China, but the proposal did not gain any traction, stonewalled by the Chinese position that the CTBT should by itself be sufficient. In any case, no focused efforts were pursued in this regard as the priorities for the P-5 were different at that time.

After the failed ratification in the United States and the slow sunset of arms control during the Bush Administration, Russia tried to keep the United States engaged and interested. The Assistant to the Russian President on Issues of Strategic Stability, Igor Sergeyev, addressing
the 2nd Article XIV Conference, suggested a range of transparency measures. In particular, he stated:

In order to strengthen the confidence-building measures after entry into force of the Treaty we are prepared to suggest, to the United States in the first place, considering the possibility to develop additional verification measures for nuclear test ranges going far beyond the Treaty provisions. This could include the exchange of geological data and results of certain experiments, installation of additional sensors, and other measures.27

This proposal, however, fell on deaf ears in Washington. To reverse strategic disengagement, this proposal could be reintroduced with a view to addressing the issue of low-yield test explosions.

At the same time, there may be several reasons why the Russian side could be reluctant to pursue these additional transparency measures. First of all, Russian experts visited the Nevada Test Site under the framework of the Joint Verification Experiment, while U.S. scientists have been only to the now-closed Semipalatinsk Test Site, but not to Novaya Zemlya. Thus, Russia may view possible access to Novaya Zemlya as a major trump card that requires sufficient stimuli to entice cooperation.

Secrecy is deeply rooted in the Russian strategic culture. At the same time, Russia tends to deliver statements aimed at domestic and international audiences, which should confirm Russia’s status as a great power with nuclear weapons and nuclear technology being among its attributes. Thus, the second reason has to do with the current status of the Novaya Zemlya Test Site and the question of how much activity is actually taking place there.

The last of the 132 nuclear tests on Novaya Zemlya was conducted at the Gulf of Matrochkin Shar in October 1990. Since 1995, the test site has been used for subcritical and non-nuclear tests to confirm the safety and reliability of Russia’s nuclear arsenal. In 2006, it was reported that up to six such tests were conducted annually.28 On several occasions Russian officials asserted that the test site maintained its level of preparedness.29

The situation, however, is very different from the past when the test site was actively used. The garrison has declined from more than 15,000 people to 2,940 for the total population of Novaya Zemlya as of January 1, 2010 according to the most recent census data.30 It is also reported that the only active unit at the test site is the science-experiment department, which mostly monitors the radiological situation at the site.31 There have been no high-level visits to Novaya Zemlya since 2006 when Minister of Defense Sergei Ivanov and Rosatom Director Sergei Kirienko visited the test site. The fact that one-star General Yuri Sokolov was replaced in 2010 by Colonel Alexander Kapelko as the head of the test site further testifies to the decreased role of Novaya Zemlya within the Russian nuclear weapons complex.32

Russia has recently increased its military presence in the Arctic following President Putin’s decision to expand operational capabilities in the region in the light of potential competition for natural resources.33 It seems, however, that under the conditions of the nuclear test ban, and when the country’s only test site is located in a region that is not even accessible year round, the costs of maintaining infrastructure for nuclear test explosions are prohibitively expensive. Although the head of the test site Colonel Andrey Sinitsyn stated that Russian nuclear weapons labs continue to conduct “non-nuclear explosive experiments,”34 referring most likely to hydrodynamic and subcritical tests not prohibited by the CTBT, the main work on maintaining Russia’s nuclear arsenal appears to have shifted to nuclear weapons labs, such as in Sarov. It seems, at least, that the Russian weapons designers are facing the same problems that their U.S. colleagues and are looking in the same direction for answers. For instance, Rosatom announced development of a laser similar to but more powerful than that in the Lawrence Livermore National Laboratory in the United States, with the same purpose of ensuring the safety and reliability of Russia’s nuclear weapons.35

Another possible venue for cooperation is transparency in nuclear weapons facilities. As Russian and U.S. scientists have engaged in productive cooperation and visits for more than two decades, more formal approaches in terms of the CTBT-related measures could be explored. One such measure could be some kind of ad hoc inspections to declared nuclear weapons facilities to verify the purpose of the declared sites. Experience with the implementation of the Chemical Weapons Convention and its verification regime may be useful in this regard.
It is important to note, however, that both test site and facility transparency would have to be pursued outside of the scope of the CTBT and be limited only to NWS due to proliferation concerns. At the same time, the Open Sky Treaty, which allows overflying of the participating member-states by specifically equipped airplanes, could be implemented in regards to the test sites to provide a certain degree of transparency for the NNWS.

CONCLUSION

Cooperation on nuclear issues has been at the center of the U.S.–Russian reset policy, but with the Prague Disarmament Agenda stagnating and tensions rising between Russia and the United States on one side and China and the United States on the other, it is becoming crucial to find points of engagement. Now, when a START Treaty successor seems to be a pipedream and any attempts to restart discussion on tactical nuclear weapons would not achieve much momentum, the CTBT may provide a context for promoting multilateral cooperation in the nuclear field. Possible additional contributions from Russia and China could facilitate U.S. ratification of the CTBT and have positive spillover on relations between the countries in general. Suggested measures vary in practicality and political symbolism, but additional transparency between the three countries in the field of a test ban could foster a better climate of trust and enhance strategic stability through predictability and insurance against nuclear surprises from any of the three countries.

NOTES

* The views expressed in this paper do not represent any official views or position of the CTBTO. All opinions, errors, omissions, etc. are solely the responsibility of the author. The author would like to acknowledge the generous support of the Program on Strategic Stability Evaluation (POSSSE) sponsored by the Carnegie Corporation of New York in conducting research for this article.


8 A larger focus on Russia rather than China probably to some extent reflects the persisting Cold War mentality, which makes it easier to target a “known enemy” rather than a country on which little confirmed data exists.


10 Interestingly, during the CTBT negotiations, the Russian side pointed that because of the sandy nature of the geological deposits near the Nevada Test Site an IMS seismic station should be located much closer to meet the detection requirements.
For more on the CTBT verification regime, see [http://www.ctbto.org/verification-regime/], last accessed August 28, 2014.

Interview with a former Russian CTBT negotiator, November 2011.


See “Station Profiles,” CTBTO public website, [http://www.ctbto.org/verification-regime/station-profiles/].


Ibid., p. 40.


Interview with a former Russian CTBT negotiator, November 2011.


Slipchenko, ibid.

Litovkin, ibid.


Leskov, ibid.


Development of national regulations supporting nuclear materials control and accounting and physical protection is an important part of the broader effort to ensure states’ compliance with the requirements of United Nations Security Council Resolution 1540. This work is also promoted by the International Atomic Energy Agency, as well as within the framework of Nuclear Security Summits. Nuclear newcomers and states that have a less developed national nuclear security regulatory infrastructure often resort to foreign experience and/or international assistance to support development of their national regulations governing nuclear material control and accounting, and physical protection. While fundamental principles of nuclear security are universal, specific implementation that must be captured in national regulations and executed through national institutional infrastructure varies depending on the wide array of in-country environments.

Those involved in development of national regulations can learn several lessons from the experience of developing nuclear security regulations in Russia, Ukraine, and Belarus with U.S. support. First, the regulatory environment in each country is unique. Direct transfer of existing requirements and best practices from other countries (e.g., United States or Russia) or model requirements developed by the IAEA might lead to inability to achieve the desired nuclear security goals. Analysis of the local environment and practices and proper adjustment of model regulatory documents are critical. Second, actual regulation development constitutes formalization of accumulated best practices. Clear understanding of regulation content is critical before regulation development starts. Best practice exchanges involving both national authorities and nuclear facility operators play an important role in achieving this understanding. Third, it is impossible to regulate every aspect related to nuclear security. In general, a rather limited set of mandatory requirements supported by proper enforcement must be supplemented with sound management practices and an adequate nuclear security culture. The right balance would ensure that all critical requirements are met, yet give operators sufficient flexibility in their approach to compliance with mandatory requirements. This paper reviews experience in supporting development of nuclear regulations in Russia, Ukraine, and Belarus and outline strategies that can be used by states developing their national nuclear security regulations as well as states and organizations supporting them to enhance the regulatory development process.

INTRODUCTION

Regulations are key to reliable nuclear security. Regulations establish the goals for nuclear security activities, define the responsibilities of the entities and individuals involved, and provide guidance regarding implementation of the responsibilities. Regulations also capture existing best practices, ensure uniformity in their implementation, and provide criteria to evaluate performance and compliance.
Development of national regulations supporting nuclear materials control and accounting and physical protection is an important part of the broader effort to ensure states’ compliance with requirements of United Nations Security Council Resolution 1540, as well as other international regimes applicable to nuclear security, including the Convention on Physical Protection of Nuclear Material and IAEA Safeguards. Development of nuclear security regulation is promoted by the International Atomic Energy Agency, within the framework of Nuclear Security Summits, as well as other multilateral or bilateral cooperative efforts.

Nuclear newcomers, states that have less developed national nuclear security regulatory infrastructure, or states that have limited resources often resort to foreign experience and/or international assistance to support development of their national regulations governing nuclear material control and accounting and physical protection. There are multiple examples of international assistance efforts aimed at developing nuclear security regulations:

- The IAEA issues multiple recommendations that provide advice on the development of national regulatory infrastructure as a whole, as well as model content for domestic nuclear security regulations. The most notable example is INFCIRC/225/Rev 5, “Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities.”

- As part of its International Physical Protection Advisory Services the IAEA reviews the national nuclear security regulations of the host country, provides recommendations on improving them, and provides additional follow-up assistance, if requested by the host country.

- Since the 1990s the United States and other international donors have provided significant support to the Former Soviet Union states—Russia, Ukraine, and Belarus in particular—in developing national nuclear security regulations. This support has included financial assistance to pay for the work of experts involved in development of regulations, as well as subject matter expertise on issues related to the scope of regulations under development.

The U.S. regulatory development support to Russia, Ukraine, and Belarus has resulted in the enactment of several dozen regulations ranging from high-level requirements captured in laws, government decrees, federal norms, and rules through detailed technical guidelines providing implementation recommendations to nuclear security personnel at nuclear sites. Due to its scope, the U.S. regulatory development cooperation with Russia, Ukraine, and Belarus presents valuable experience and can provide multiple lessons to those beginning development of national nuclear security regulations.

**REGULATORY ENVIRONMENT IN RUSSIA, UKRAINE, AND BELARUS**

While fundamental principles of nuclear security are universal, specific implementation that must be captured in national regulations and executed through national institutional infrastructure varies depending on the wide array of in-country environments. For the purpose of this paper, it is important to understand regulatory environment in Russia, Ukraine, and Belarus that impacts development of nuclear security regulations. While all three countries have the legacy of the Soviet Union, they have their own specifics that explain differences in regulations development.

**RUSSIA**

Russia has inherited a vast nuclear industry from the Soviet Union. It includes:

- a nuclear weapons complex;
- a full range of nuclear fuel cycle enterprises from uranium mining through spent fuel reprocessing and disposition;
- several dozen nuclear power reactors;
- multiple nuclear research facilities;
- a nuclear-powered fleet, including icebreakers, nuclear powered civilian and navy surface ships, and nuclear submarines;
intensive transportation of nuclear materials;

- a significant cadre of nuclear industry personnel with skills and experience comparable to those of other leading nuclear nations;

- supporting organizations, including R&D institutes, equipment manufacturing and construction enterprises, and others.

The inventory of nuclear materials in Russia includes several hundred tons of highly enriched uranium and weapons grade plutonium. From the standpoint of the regulatory system, it is worthwhile noting the following specifics:

- Russia inherited a significant regulatory basis from the Soviet Union. This regulatory basis does not always support nuclear security best practices. Changing available regulations requires significant time and effort. Changing implementation practices and providing operators with the capability to comply with new regulations require even greater time, effort, and resources.

- The availability of civilian and defense nuclear complexes results in two separate regulatory systems, including two independent nuclear regulatory bodies. There are regulations that apply to both civilian and defense nuclear industry applications and regulations that apply to only the civilian or defense part. Overall, civilian nuclear applications are better covered with necessary regulations, including nuclear security, than defense applications. For example, there is still no federal law governing the use of nuclear energy for defense purposes.

- Russia has a poor tradition of independent regulation. Independent nuclear regulatory body in Russia was created only in 1991. Rather than having strong federal legislation supported with regulations issued by an independent regulatory body, Russia has significant regulatory development authorities inherited by or delegated to agencies managing the use of nuclear applications, i.e. separation of regulator and operator is not always sufficient and may lead to a conflict of interest. The situation has gradually been changing since the early 1990s, but significant work is still to be done.

- Russian regulations are very prescription based rather than performance based. Under a performance-based system, security critical mandatory requirements would be established in federal legislation or by an independent regulator. Operators will then be given flexibility to choose their own way of ensuring compliance with mandatory regulations, while the regulator can issue voluntary recommendations supporting implementation. In the prescriptive-based system existing in Russia, mandatory requirements are often very detailed and prescribe even minor implementation details. Again, some changes have occurred in this area as well, but the situation is often complicated by the fact that operators are used to very detailed mandatory guidance and not prepared to bear significant responsibility for developing their own approach to ensure compliance.

- There are multiple agencies with functions related to nuclear security. This leads to the need to ensure interagency coordination in nuclear security activities.

As a nuclear weapon state Russia is exempt from multiple nuclear security related international obligations, such as IAEA safeguards, that impose certain requirements on and drive certain developments in national regulations.

UKRAINE

The Ukrainian nuclear industry is not as comprehensive as its Russian counterpart. Nevertheless, Ukraine has 15 operational nuclear power reactors, most of them commissioned when Ukraine was part of the Soviet Union, several nuclear research facilities, and significant supporting infrastructure. Until recently, Ukraine had a stock of highly enriched uranium that was removed from the country as part of the joint U.S.-Russian effort. Ukraine also has qualified personnel capable of supporting nuclear industry operation, including nuclear security.

While Ukraine also had inherited Soviet regulatory structures, due to the relatively smaller nuclear industry and absence of a defense component, it has greater flexibility in adjusting its regulations and implementation practices compared with Russia. Changes were also driven by the fact that Ukraine joined the Nonproliferation Treaty as a non-nuclear weapon state and...
therefore has to accept IAEA safeguards and implement regulatory changes supporting
compliance with safeguards obligations. Interagency coordination in Ukraine is also easier as
the number of agencies involved is smaller than in Russia.

BELARUS

There is only one nuclear facility that was built during the Soviet time—a research nuclear
reactor that uses highly enriched uranium (HEU). An effort was made to remove HEU from
Belarus but this has not been successful so far due to disagreements between the United
States and Belarus. Another nuclear facility—a nuclear power plant—is now under construc-
tion with Russian support. Commissioning of the first reactor is expected in 2018 and the
second in 2020. An independent nuclear regulatory body exists in Belarus as a department
within the Ministry of Emergency Situation, which also has multiple other functions not
related to nuclear safety and security regulation. Until recently, this regulatory body was
understaffed, with only one staff member having physical protection and nuclear materials
control and accounting as part of his daily responsibilities. Construction of the nuclear power
plant resulted in positive development, including an increase in regulatory staffing, but
significant effort still needs to be made to provide appropriate support.

Adequate nuclear security regulations had been almost non-existent in Belarus until the U.S.
regulatory development support began. This support resulted in the development of several
fundamental regulations governing physical protection and nuclear materials control and
accounting. Belarus is also a non-nuclear weapon party to the Non-Proliferation Treaty and
has a safeguards agreement with the IAEA that is supported by several national regulations.

LESSONS LEARNED FROM REGULATORY DEVELOPMENT COOPERATION IN RUSSIA,
UKRAINE, AND BELARUS

While there are still some gaps in regulatory coverage of nuclear security in Russia, Ukraine,
and especially Belarus, the cooperation has been mostly successful and has resulted in the
development of much needed regulations. This cooperation had to overcome multiple
obstacles and provide valuable lessons to those beginning development of their national
nuclear security regulations.

UNDERSTANDING THE REGULATORY AND OPERATIONAL ENVIRONMENT

While fundamental principles of nuclear security are universal, specific implementation that
must be captured in national regulations and executed through a national institutional
infrastructure varies depending on the wide array of in-country environments. The regulatory
and operational environment in each country is unique. Direct transfer of existing require-
ments and best practices from other countries (e.g. the United States or Russia) or model
requirements developed by IAEA might lead to inability to enact the necessary regulations
and achieve desired nuclear security goals. Analysis of the local environment and practices
and proper adjustment of model regulatory documents are critical.

The U.S. regulatory development support in Russia failed to achieve an appropriate
enactment rate of the developed regulations. Multiple regulations were developed, but not
properly enacted to become mandatory for operators. Changes were made to cooperation
implementation to take into account specifics available in Russia which led to the enactment
of all but a few regulations that were developed within cooperation.

The following are examples of regulatory and operational environment factors that sig-
nificantly impacted implementation of regulatory cooperation in Russia:

- The Law on Technical Regulation that was enacted in late 2002 significantly changed
requirements to the procedure of establishing mandatory requirements in multiple
areas, including physical protection and nuclear materials accounting and control.
Implementation of cooperation was adjusted and significant attention is given to the
regulatory authority of the organization developing specific regulation and regulation
content to ensure compliance with the requirements of the Law on Technical
Regulation. This situation was complicated by the fact that multiple substantive amendments were introduced to the Law after its enactment.

- The regulatory authorities of Roschtechnadzor—Russia’s nuclear regulatory body participating in cooperation—were changed several times. At some point Roschtechnadzor was placed under the Ministry of Natural Resources and Environment and its authority to enact federal norms and rules—the highest level of mandatory nuclear regulation—was transferred to the Ministry as well. This affected cooperation, as Roschtechnadzor was still in charge of developing regulations, but had to submit them to the Ministry for enactment. Later the situation was reversed and the Roschtechnadzor authority was restored.

- Enactment of high-level Russian regulations requires reconciliation with multiple agencies, including those that are not directly related to nuclear security and not involved in cooperation. Reconciliation of two high-level documents in the area of PP and MC&A—“Rules of Physical Protection of Nuclear Materials, Nuclear Facilities, and Nuclear Material Storage Sites” approved by the Government Decree and Federal Norms and Rules “Basic Rules of Accounting and Control of Nuclear Materials”—took more than a year after the final drafts were developed.

- Armed guards at most nuclear sites in Russia, Ukraine, and Belarus are provided by Internal Troops of the Ministries of Internal Affairs (MVD IT) of the respective countries, not by private pro-force contractors as in the United States. MVD IT is independent from the operator and managed by a separate government agency. As an essentially military organization, MVD IT has a different mode of operation, approaches, organization of its activity, and personnel training. Requirements for the physical protection of nuclear sites must be reconciled with the MVD at the level of regulations applicable to all sites and with the specific MVD IT unit related to the organization of protection at a specific nuclear site.

**DEVELOP CAPABILITIES BEFORE ESTABLISHING REGULATORY REQUIREMENTS**

Operators need to be capable of complying with established requirements. If requirement is established without operators being capable of such compliance, then either the requirement would not work in the case of loose enforcement or operators would have to stop their activity due to inability to comply with an established mandatory requirement. Necessary capabilities may include additional personnel or new skills for available personnel, resources to modify facilities and upgrade equipment, and time to adjust operations to new requirements.

In a natural way, if something new is introduced, it passes through stages from innovation to best practice and the widely acceptable practice captured in a voluntary standard, and finally the mandatory requirement captured in regulation. When regulation establishing a mandatory requirement is developed with foreign support, it is often the case that the donor has significant experience in implementing this requirement, while the recipient has insufficient capability to ensure compliance.

In this case, it is important to accompany development of regulation with development of appropriate compliance capabilities. Examples from the regulatory cooperation with Russia, Ukraine, and Belarus listed below support this point:

- Russia’s Basic Rules of Accounting and Control of Nuclear Materials were first introduced in the late 1990s and then revised twice, in 2006 and 2012. Each following revision saw an increased strength of requirements. This was due to the fact that Russia’s nuclear facilities capabilities of complying with new requirements grew over time. The work on developing this regulation was complemented by activities aimed at developing capabilities to comply with it, including personnel training, equipment supplies, site upgrades, measurement methodologies development, and so on. On the other hand, certain requirements were not introduced in the latest revision and were postponed for future consideration due to the inability of a large share of Russian nuclear sites to comply with them. We can observe a similar pattern with other regulations as well.

- Training on vulnerability analysis delivered to Belorussian nuclear security personnel proceeded to the development of Belarus national regulation on vulnerability analysis.
A clear understanding of regulation content is critical before regulation development starts. Best practice exchanges and training activities involving both national authorities and nuclear facility operators play an important role in achieving this understanding and should become a key part of international nuclear security assistance. In their own turn, national stakeholders should consider development of capabilities to comply with nuclear security requirements as their highest priority.

DO NOT OVERREGULATE

As discussed above, different countries have different regulatory cultures. Some countries issue very detailed regulations that prescribe even minor details for implementing regulated activities. Other countries establish more general mandatory requirements covering safety and security-related issues, while allowing operators significant flexibility in ensuring compliance. In any case, it is impossible to regulate every aspect related to nuclear security.

In Russia a relatively limited set of documents establishing mandatory requirements for physical protection and nuclear materials control and accounting has been developed. The majority of documents constitute so-called “methodological recommendations” or “safety guidelines.”

These are non-mandatory documents outlining one of the ways to ensure compliance with mandatory requirements. When the agency that issued these non-mandatory document inspects compliance with mandatory requirements it considers them as a preferable method of compliance, meaning that a site that uses this method is automatically considered to be in compliance. This does not mean that the site is not allowed to choose its own method. However, it needs to provide justification supporting the fact that an alternative approach also ensures compliance with mandatory requirements. Within this framework, most of the smaller sites in Russia use approaches established in methodological recommendations. Larger sites that have sufficient capability often choose their own approach and justify it to the controlling authority.

On the other hand, in countries that are new to modern nuclear security practices the level of nuclear security culture might be low and mandatory requirements would be the only way to ensure achievement of nuclear security goals.

In general, a rather limited set of mandatory requirements supported by proper enforcement must be supplemented with sound management practices and an adequate nuclear security culture to ensure achievement of nuclear security goals.

CONCLUSIONS

Experience of regulatory development cooperation in Russia, Ukraine, and Belarus provides multiple valuable lessons to those beginning development of their national nuclear security regulations and the international parties supporting them. This paper has reviewed the experience of cooperation and identified lessons learned.

- First, the regulatory environment in each country is unique. Direct transfer of existing requirements and best practices from other countries (e.g. the United States or Russia) or model requirements developed by the IAEA might lead to inability to achieve the desired nuclear security goals. Analysis of the local environment and practices and proper adjustment of model regulatory documents are critical.

- Second, actual regulation development constitutes formalization of accumulated best practices. Clear understanding of regulation content is critical before regulation development starts. Best practice exchanges involving both national authorities and nuclear facility operators play an important role in achieving this understanding.

- Third, it is impossible to regulate every aspect related to nuclear security. In general, a rather limited set of mandatory requirements supported by proper enforcement must be supplemented with sound management practices and adequate nuclear security culture. The right balance would ensure that all critical requirements are met, yet would give operators sufficient flexibility in their approach to compliance with mandatory requirements.
The following recommendations to those starting development of national nuclear security regulations either independently using international recommendations, such as IAEA’s recommendations on physical protection, or with foreign assistance can be made based on identified lessons:

- Analyze the regulatory environment and identify stakeholders and procedures critical for successful development of a regulation. Based on the results of analysis, develop a road map for regulation development and follow it during development of regulations. In addition to nuclear security experts involve local legal experts from the early stages.

- When transferring nuclear security best practices, do not insist on copying them. Instead, capture the nuclear security goals to be achieved, analyze the local practices contributing to the achievement of these goals, and adjust best practices to ensure buy-in of the local stakeholders and personnel.

- Ensure that national stakeholders have sufficient capabilities to comply with newly established regulatory requirements. If capabilities are not sufficient, start the capabilities development effort before or at least no later than actual regulation development. Capability development may include personnel training, best practices exchange, equipment supplies, site upgrades, etc.

- Do not try to regulate everything up to the minor implementation details. Proceed from a performance-based approach to ensure a balanced mix of nuclear security critical mandatory requirements, supporting implementation guidelines, sound management practices, and a nuclear security culture.

NOTE

The new basic level of the iSI International Security Index for 2014 at the beginning of the year was set at 3,205 points, up 60 points on the previous year. The increase reflected subsiding military-political tensions on the Korean peninsula, a reduced threat of a foreign intervention in the Syrian conflict, and the progress achieved at the Iranian talks. The new basic level of the iSI index stood 1005 points below the ideal level of international security, which equals 4,210 points, in accordance with the methodology of calculation. The ideal level is defined as a state of affairs when nothing threatens international security. The closer the actual level

Andrey Kortunov, Director General, Russian Council for Foreign Affairs—by phone from Moscow: The level of security in the world and especially in our region declined in summer 2014. The main factor here was the Ukrainian crisis and the impact that it had on relations between Russia and the United States, and Russia and Europe. In addition to the immediate consequences (the destabilization of states in the center of Europe, military clashes), the infrastructure of military-technical and military-political cooperation between Russia and the West also became a victim of the crisis. In my opinion, this is the most serious security challenge to regional security.

Positive developments of the period included the dialogue on the Iranian nuclear issue continuing despite all existing difficulties. A relatively successful presidential election that took place in Afghanistan should also be mentioned here. It does not guarantee security so far, but it was a definite success for the country and neighboring region. The tensions on the Korean peninsula have also slightly reduced. The situation in the DPRK, though poorly understood, is probably under the government's control.
of the iSi to the ideal level, the better the international security situation is, and vice versa. The basic level of the index stood at 3,228 points in 2010, 3,284 points in 2011, 3,115 points in 3115, and 3,145 points in 2013.

Despite the increase in the basic yearly level of the iSi, the year 2014 began with volatile trends. The index rose from 2812 points on January 1, 2014 to 2863 points on February 1 to reflect continued progress at the talks with Iran, the OPCW operation to destroy Syrian chemical weapons, and the launch of peace talks between the parties to the Syrian conflict and international mediators.

By the end of February, however, tensions began to spiral in the southeastern regions of Ukraine. The United States and the EU imposed sanctions on a number of Russian officials and companies over the decision to accept Crimea and Sevastopol as members of the Russian Federation. There was also continued instability in the Middle East, and mounting tensions on the Korean peninsula and in Latin America. By March the iSi index had fallen to 2,844 points, 19 points down from the February 1 level. It then fell further to 2,815 points by April 1, 2,796 points by May 1, and 2,776 points by June 1, to reflect a sharp deterioration of the international military and political situation.

- **Former Soviet States.** Military-political tensions that broke out in Ukraine in the winter and spring of 2014 became the paramount threat to regional and international security.

There were violent clashes between the police and protesters in Kiev in January and February over the Ukrainian government’s decision to suspend the signing of an Association Agreement with the European Union; over 100 people were killed. On February 21, the government of Viktor Yanukovych and the leaders of the Ukrainian opposition reached an agreement to settle the crisis by holding an early presidential election and reinstating the 2004 version of the Constitution, thereby curtailing presidential powers. On February 22 the Ukrainian parliament voted for the ousting of President Yanukovych and ordered the release of former prime minister Yuliya Tymoshenko from jail. Parliament speaker Oleksandr Turchynov was appointed as acting president.

On March 21 the new government in Kiev signed the political section of the Association Agreement with the EU.

In late February and early March the situation began to deteriorate in the southeastern regions of Ukraine. On February 26 Crimea saw rallies by the supporters and opponents of the new Ukrainian government; protesters seized several government buildings. On February 27 the Crimean parliament ordered a referendum on the autonomy’s status. The referendum was held on March 16; a majority of Crimeans voted in favor of the peninsula becoming part of Russia. On March 18 the Russian President signed a bill granting Crimea and the city of Sevastopol the status of members of the Russian Federation. Kiev responded by halting water supplies to Crimea via the Crimean Canal from mainland Ukraine.

In response to Crimea once again becoming part of Russia, the United States and the EU imposed sanctions on several Russian officials and companies; cancelled the Russia–EU summit that was scheduled for June 3; and suspended talks with Russia on the liberalization and lifting of the visa regime. Members of the G7 suspended preparations for a summit in Sochi. The UN Security Council convened on several occasions to discuss the situation in Ukraine. On March 27 the UN General Assembly passed a resolution on Ukraine’s territorial integrity.

---

**Pál Dunay (Hungary),** Director of OSCE Academy in Bishkek—by **e-mail from Bishkek:** The Ukrainian conflict and its inter-state aspect cannot be maintained in the longer run. The politico-military crisis will give way to a humanitarian crisis soon. The fast rising number of asylum seekers from the Donetsk and Lugansk areas both to Russia and to other parts of Ukraine will burden both states. Both states (although on very different level) are stripped of resources, Russia has no GDP growth (contrary to 2012 when it had 4.3 per cent), and Ukraine will have a disastrous year coming economically as well. Will it contribute to internal destabilization? This is a question difficult to respond to but certainly not irrelevant.
On March 29 an assembly of the Crimean Tatar people held in Bakhchisaray approved the decision to begin the formation of national territorial autonomy in Crimea.

Meanwhile, protests continued in eastern parts of Ukraine; the protesters demanded a referendum on the country’s federalization and seized several government buildings. The authorities in Kiev accused Moscow of supporting the protesters in eastern Ukraine, and launched a security operation involving the use of force to suppress the protests. On April 5, the NATO Parliamentary Assembly suspended cooperation with Moscow. On April 10 PACE voted to strip the Russian delegation of its vote until the year’s end, and threatened to expel Russia from all the governing bodies of the assembly. The United States and the EU threatened fresh sanctions. Russia, the United States, the EU, and Ukraine held talks on April 17 in Geneva; they agreed a plan to settle the Ukrainian crisis, but the rallies by the supporters of federalization in eastern Ukraine continued. On April 24 Russia began military drills close to the Ukrainian border.

On May 2, 46 people died in Odessa during clashes between the supporters and opponents of the new government in Kiev and the ensuing blaze in the Trade Unions Building. A referendum on self-determination was held in May in Donetsk and Lugansk Regions, but the authorities in Kiev refused to recognize it. The United States and the EU imposed further sanctions on Russia over the situation in eastern Ukraine.

On May 25 Ukraine held an early presidential election; Petro Poroshenko won in the first round and on June 7 the new President of Ukraine took office. On June 15 under Lugansk the militia shot down an airplane with Ukrainian military on board. This led to protests and attacks at the Russian Embassy in Kiev. On June 20 Mr Poroshenko announced a temporary ceasefire in the southeast of the country.

On June 10 negotiations between Russia, the EU, and Ukraine on Russian gas supplies to Ukraine were completed with no result. On June 27 Ukraine, Moldova, and Georgia signed the economic part of the association agreement with the EU.

The iSi Index was also depressed by the situation in other post-Soviet countries.

There was an exchange of fire between Kyrgyz and Tajik border guards on the border between the two countries on January 14; seven people were injured.

Kazakhstan saw protests in February over the devaluation of the national currency.

The United States began to remove hardware from its airbase in Kyrgyzstan in early March.

The Kazakh and Armenian cabinets resigned in April.

Mass riots broke out in Tajikistan’s Gorno-Badakhshan Autonomous Region in May after the killing of several local residents by police officers during a counternarcotics operation.

On May 29 Russia, Belarus, and Kazakhstan gathered in Astana to sign a treaty on the establishment of the Eurasian Economic Union.

Middle East and Africa. The situation in the Middle East and Africa continued to exert downward pressure on the iSi Security Index in the winter and spring of 2014.

A civil war raged on throughout Syria. There was fighting between government troops and the rebels in Damascus, Aleppo, Adra, Homs, and on the border with Lebanon. In February militants of the Jund al-Aqsa group attacked the Alawite town of Maan near Hama, killing more than 20 civilians. Fighting also intensified between the rival groups of Syrian rebels. In early January the Syrian government and the National Coalition of Revolutionary and Opposition Forces officially confirmed their participation in the Geneva 2 peace conference. Two rounds of talks involving the parties to the conflict and international mediators were held in Geneva with no result.

In the spring of 2014 fighting continued between government troops and the Syrian opposition on the southern and eastern outskirts of Damascus, in Latakia, the town of Tabqa on the river Euphrates, and in Kalaat El Hosn. Registration of candidates in the Syrian presidential election began in April. On May 13 Lakhdar Brahimi resigned from the post of special UN representative for Syria.
In June fighting between the army and the rebels took place in Damascus and Aleppo; the army recaptured the city of Kesap from the Islamists and took control over the village of Tfila on the Syrian-Lebanese border. Bashar al-Assad won the presidential election, held on June 4; Western countries did not recognize the legitimacy of the election.

In the winter of 2014 the situation with the Iranian nuclear program reached a degree of stability following the deal agreed in November 2013 by the six international mediators and Tehran. After negotiations held in Vienna in February and April 2014, Iran and the international mediators agreed the approaches to drawing up a comprehensive agreement on the Iranian nuclear program. In May, however, the parties failed to agree on the draft of such an agreement. Meanwhile, the IAEA said in a report that Iran had destroyed half of its stockpile of uranium enriched to 20 percent.

In Geneva and in Vienna in June talks between Iran and international mediators on the nuclear problem of the country were held; no comprehensive agreement was achieved.

**Evgeny Satanovsky (Russia),** President of the Institute of Middle East Studies—by phone from Moscow: Iran and the six international mediators at the latest negotiations in Vienna failed to agree the text of a comprehensive agreement on the Iranian nuclear issue. An agreement could be reached either if the parties are ready to sign and turn a blind eye to the fact that it will never work, or if the West agrees to all of Iran’s conditions. Iran will never give up its nuclear program. To hope that this could happen one day is pointless and unprofessional.

**Abdulaziz Sager (Saudi Arabia),** Chairman and Founder of the Gulf Research Center—by e-mail from Dubai: Saudi Arabia continues to play the key role in providing stability to global energy markets. As such, the kingdom has issued a statement indicating that it is ready to supply the markets with additional oil in case the crisis over the Ukraine must impact those markets negatively. From an energy perspective, this is a development that is being closely watched by Saudi officials.

The government of Egypt officially designated the Muslim Brotherhood as a terrorist organization, much to the anger of the Islamists’ supporters. Clashes continued between the police and Islamist protesters in the winter and spring of 2014. There were also several terrorist attacks. On January 14 Egyptian voters approved the draft of a new constitution at a referendum. On February 24 the interim government stepped down. On May 26–28 the country held a presidential election. Former Defense Minister, Field Marshal Abdel Fattah al-Sisi, won in the first round and in June was inaugurated as the country’s president.

In Iraq, Islamist groups seized the towns of Fallujah and Ramadi in early January. Fighting continued between the Iraqi security forces and the Islamic State of Iraq and the Levant (ISIS) in the winter and spring of 2014. In April government forces conducted a large counter-terrorism operation. In June the military-political situation deteriorated sharply.

**Halil Karaveli (Turkey-Sweden),** Senior Fellow with the Central Asia-Caucasus Institute & Silk Road Studies Program Joint Center—by e-mail from Stockholm: The advancement of ISIS and the de facto disintegration of Iraq have contributed to the further de-escalating of tensions between the United States and Iran, since these two powers share a common interest in countering the Sunni radicalism and providing the territorial integrity of Iraq. So paradoxically, the advances of ISIS also have a geopolitical positive sideeffect—an improvement in relations between the two countries. This can improve the overall security climate in the region as a whole.
Militants of the group Islamic State of Iraq and the Levant captured big parts of the territory in the northwest of the country; the authorities announced a general mobilization. The United States expressed willingness to help the government in Baghdad in the fight against extremists.

Turkey saw large anti-government protests in January over new laws tightening government control over the Internet. The country held municipal elections on March 30. The ruling Justice and Development Party led by President Recep Tayyip Erdogan won a majority of the vote.


On April 23 Palestine’s Fatah and Hamas movements agreed to form a government of national unity. Israelis responded by suspending talks with the Palestinians. During June, the Israeli Air Force launched a series of attacks on the Gaza Strip in response to rocket fire into its territory.

The government of Libya announced a state of emergency on January 19 over continuing inter-tribal clashes. In mid-February the country saw protests calling for a dissolution of the interim parliament and early elections. On March 14 the UN Security Council extended the mandate of its mission in Libya by another 12 months.

Libyan Prime Minister Abdullah al-Thinni resigned in April. On May 5 the Libyan parliament elected his successor, the businessman Ahmed Maiteeq. The move failed to end the clashes between the security forces and Islamists. Supporters of the opposition general Khalifa Haftar staged a mutiny against the interim government in mid-May. The authorities made concessions and suspended parliament. In June the government led by Ahmed Maiteeq had been recognized as unconstitutional; clashes broke out between supporters and opponents of the disgraced general Haitham Haftorah. On June 25 parliamentary elections were held in the country.

Yemen saw clashes in late January between the Shia group El-Husi and Salafi Muslims. Shia forces seized the town of Khut and the village of Khamri. On February 4 Shia and Sunni forces signed a ceasefire agreement, but intertribal clashes continued throughout the country. Close to 60 Al Qaeda militants were killed in a spring counterterrorism operation. In June, clashes occurred between the governmental forces and insurgents; about 120 people were killed.

The Central African Republic saw clashes between Christians and the Muslim rebel movement Seleka. On January 10, President Michel Djotodia stepped down. On February 10 the EU approved a CAR military mission. In April soldiers from Chad killed 30 peaceful civilians. In June, because of sectarian clashes 50 people were killed.

In South Sudan, supporters of former vice-president Riek Machar staged a coup attempt in the winter. Three peacekeepers were killed in an attack on the UN mission compound. Direct peace talks began between the government and the rebels in January. In April the parties signed an agreement to settle the ethnic conflict.

In Nigeria, Boko Haram rebels attacked several towns and villages in April, kidnapping a large group of schoolgirls and killing 60 people.

In Algeria, protests broke out in February and March against President Abdelaziz Bouteflika’s decision to run for another term of office. Nevertheless, Bouteflika was re-elected on April 17.

There were riots in South Africa after parliamentary elections in May. Terrorist attacks took place multiple times in the winter and spring of 2014 in Iraq, Palestine, Afghanistan, the Sinai Peninsula, Egypt, Lebanon, Yemen, Somalia, Libya, Syria, Thailand, Nigeria, India, China, and Kenya.

East, Southeast, and South Asia. Though predominantly a peaceful region, if compared with the Middle East, Asia and particularly its eastern part demonstrated growth of geopolitical tension and rivalry among major regional powers; these trends also impacted the ISI dynamics.
Korean Peninsula. Tensions persisted on the Korean peninsula from winter to summer of 2014. Increased activity was detected at the North Korean nuclear testing range.

On February 12, North Korea and South Korea held their first high-level talks in seven years. On March 22, however, Pyongyang test-fired numerous short-range missiles over the Sea of Japan. On March 31 there was an exchange of fire between the two countries’ forces in the Yellow Sea. In May, North Korea held a live firing exercise near the western border with South Korea in the Yellow Sea. On June 29, North Korea launched short-range missiles toward the Sea of Japan.

In Thailand, anti-government protests continued in the winter and spring of 2014. The country held an early parliamentary election on February 2. In several provinces the voting was disrupted after opposition supporters blockaded polling stations. On March 21 the Constitutional Court declared the results of the February poll invalid. Nevertheless, the country held an election to the upper chamber of parliament on March 30. On May 7 the Constitutional Court removed Prime Minister Yingluck Shinawatra from office. On May 22 the Thai military seized power in a coup d’état.


Protests broke out in Taiwan in March against the ratification of an agreement with China on trade in services and closer economic ties.

Protesters in Vietnam called for the removal of Chinese oil drilling platforms from disputed waters around the Paracel Islands in the South China Sea.

Bangladesh held a parliamentary election on January 5. Some of the polling stations were ransacked by protesters.

Nandan Unnikrishnan (India), Vice President, Observer Research Foundation—by phone from Delhi: There is still no total clarity as to what the views of the Indian Prime Minister Narendra Modi on the foreign policy issues are. But obviously, a large set of domestic issues was accumulated, which must be solved by new leadership in the next two to three years. Those include problems of economy, the social sphere, and politics. The internal agenda of the new prime minister promises to be very intense. Emphasis on domestic issues does not mean that the new Indian government will disregard foreign policy. Rather, India’s international stance will be determined by internal affairs, which will be primarily connected to the social and economic agenda.

India held a general election in April–May 2014. The nationalist BJP party, led by Narendra Modi, won a convincing victory.

Afghanistan and Pakistan. Talks between the Nawaz Sharif government and the Taliban movement in Pakistan began in Islamabad on February 6. In Pakistan, in June the militants attacked the airport in Karachi; there were victims. The Air Force conducted a special operation in North Waziristan against the Islamists.

In Afghanistan, the Taliban staged a series of attacks against military bases and civilian infrastructure in the winter and spring of 2014. In February, 28 Taliban fighters crossed into Turkmenistan and attacked Turkmen border guards.

Afghanistan held a presidential election on April 5. Eight candidates were in the running; none of them won a majority in the first round. On June 14 the second round of the presidential election was held; presidential candidate Abdullah Abdullah refused to recognize the election results.
Nandan Unnikrishnan (India), Director of Eurasian Studies, Vice President, Observer Research Foundation—by phone from Delhi: Successful presidential elections in Afghanistan contributed a positive development to South Asian regional security. Those in India anticipate from the new President effective work towards stabilizing the Islamic Republic of Afghanistan (IRA). We hope that the new Afghan authorities will find their own way out of the complicated situation that afflicts their country and lessen the influence of the Afghanistan factor on the rest of South Asian security.

U.S. President Barack Obama announced in May that 9,800 U.S. servicemen would remain in Afghanistan after the end of the military mission in late 2014, helping to train Afghan troops and assisting in preparing counterterrorism operations.

- **European Union.** Dissatisfaction with the European governments’ economic policies remained the main cause of social disturbances and protests in the European Union. There were anti-government protests in the winter and spring of 2014 in Bulgaria, Italy, Greece, Spain, France, and the UK.

Talks on Serbia’s accession to the EU commenced in Brussels on January 21.

There were mass protests over the state of the economy in Bosnia and Herzegovina; more than 200 people were injured in clashes with the police.

The Cypriot government resigned on February 28.

The U.S. president signed a bill on raising the country’s debt ceiling on February 26.

Elections to the European parliament of the 2014–2019 convocation were held in the EU countries on May 22–25. The centrist pro-European parties won a solid majority of the vote, but ultra-right and Euroskeptic forces also made big gains.

- **Latin America.** The situation remained volatile in some Latin American countries in the winter and spring of 2014.

There were anti-government protests in Venezuela in February over the government’s economic and political strategy. They turned into clashes in the spring; several people were killed.

In Brazil, farmers rallied for agricultural reform; the rally soon degenerated into violent clashes with the police.

- **Strategic Stability and Nuclear Security.** A document on the protection of radioactive substances was signed at the Nuclear Security Summit in The Hague, Netherlands on March 25.

On May 6, 2014 representatives of Russia, Britain, China, France, and the United States signed a protocol to the treaty on the nuclear-weapon-free zone in Central Asia. The document was signed on the sidelines of the Third Preparatory Committee of the NPT Review Conference. UN Secretary-General Ban Ki-moon emphasized that the five nuclear-weapon states had undertaken an obligation to respect Central Asia’s nuclear-weapons-free status, and not to use, or threaten to use, nuclear weapons against the region’s countries.

Nikolai Zlobin (USA—Russia), President of the Center on global interests—by phone from Washington: The deterioration between the USA and Russia is just beginning, but the depth, sharpness, and the scope of the process is not yet known to us. The current U.S. administration is unlikely to work on improving U.S.—Russian relations, because it is completely unnecessary for them. The next administration in Washington will grandfather the damaged relationships and I think it will have a good chance to continue to worsen them. The same, however, is true for the Russian side.
Natural and Man-Made Disasters. A Malaysia Airlines flight to China with 239 people on board disappeared from the radar on March 8. Over 200 people died when a ferry sank in South Korea in April.

In Chile, five people were killed by a powerful earthquake and tsunami.

About 300 people died in a mudslide in Afghanistan’s northwestern province of Badakhshan.

Based on the media reports, approximately 300 people were killed in a coal mine accident in Turkey in May; the tragedy triggered anti-government protests.
BRICS—A SLEEPING GIANT IN GLOBAL ICT POLICIES?

Today the BRICS states constitute one of the most massive and rapidly growing segments of the global internet community. In 2013 the total number of internet users in BRICS states exceeded 900 million (which accounted for 38 percent of the world’s internet audience, see Table 1) while still undergoing rapid growth ranging from 10 percent to 41 percent. The total contribution of the internet sector to BRICS economies in 2013 topped 500 billion U.S. dollars, and yet forecasts say it will double by 2015. In the very near future BRICS will represent the most numerous and active part of the twenty-first century’s digital society.

<table>
<thead>
<tr>
<th>Country</th>
<th>Population as at March 2014 (thousands)</th>
<th>Number of internet users as at July 2013 (thousands)</th>
<th>World rank by number of internet users</th>
<th>Internet penetration rate, percent</th>
<th>Share of world’s internet audience, percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Brazil</td>
<td>201,032</td>
<td>99,358</td>
<td>5</td>
<td>49.4</td>
<td>4.13</td>
</tr>
<tr>
<td>India</td>
<td>1,242,580</td>
<td>151,599</td>
<td>3</td>
<td>12.2</td>
<td>6.30</td>
</tr>
<tr>
<td>China</td>
<td>1,363,780</td>
<td>568,192</td>
<td>1</td>
<td>41.7</td>
<td>23.62</td>
</tr>
<tr>
<td>Russia</td>
<td>143,666</td>
<td>75,926</td>
<td>6</td>
<td>52.8</td>
<td>3.16</td>
</tr>
<tr>
<td>South Africa</td>
<td>52,981</td>
<td>20,012</td>
<td>25</td>
<td>37.8</td>
<td>0.83</td>
</tr>
<tr>
<td>BRICS</td>
<td>3,004,039</td>
<td>915,087</td>
<td>—</td>
<td>38.8</td>
<td>38.01</td>
</tr>
</tbody>
</table>


At the same time, this remarkable statistic only stresses the underrepresentation of the BRICS states in the field of global internet governance and cyber governance. As developments in 2014 show, the forum 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 the international security and global governance field. Neither the global discussion on transition of the oversight of critical internet functions, kick-started by the U.S. Government statement from March 14, 2014, nor the attempt to set global rules to stop uncontrolled governmental surveillance of the internet which emerged and failed at the NETMundial summit in April 2014, revealed any consistent and concrete BRICS position on these issues. Even when taking the lead, the giants of the non-Western world preferred to act in their own capacity—like Brazil, which hosted NETMundial.

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 forum’s states in the global ICT sector, and their intensive cooperation in other areas, such as reform of the global financial architecture. More than that, in fact neither of the BRICS “baskets” and pillars can be truly successful without addressing the ICT issues—just because finances, economic growth, security, science, and education are today equally dependent on the internet and other digital technologies.
So on what issues should the BRICS leaders concentrate their attention today, less than a year before the summit in Ufa, in order to claim their leadership in global ICT policies?

KEY TRENDS OF 2014 IN GLOBAL INTERNET GOVERNANCE

The likely answer brings us to the transformation of the global internet governance architecture, which in 2014 was marked by several key episodes. The first refers us to the statement by the National Telecommunications and Information Administration (NTIA). On March 14, 2014 this agency in the U.S. Government structure announced the “transition of the key functions of the domain names to the global stakeholder community.” In more detail, the statement urges the start of transition of the stewardship responsibilities of the U.S. Government with regard to the functions of the Internet Assigned Numbers Authority (IANA). These critical functions include the management and maintenance of DNS system operation; since 1997 these have been performed by the Internet Corporation for Assigned Names and Numbers (ICANN) in the framework of its contract with the NTIA. The process of stewardship transition should be finished by September 30, 2015 when the contract between ICANN and the NTIA expires. However, for the moment no one has managed to provide a detailed and consensus-based vision of a new structure that would be able to exercise stewardship of the IANA functions independently and to the benefit of the global stakeholder community. Concrete proposals on that issue are now in high demand, including those from national governments and international organizations as stakeholders.

The second key trend of 2014 in the internet governance field indicates mention of major meetings and forums on these issues. One of them is the Global Stakeholder Meeting on the Future of Internet Governance (NETmundial), which took place in Sao Paulo, Brazil on April 23–24, 2014. The meeting, which was organized in response to the “Snowden scandal,” was regarded as a chance to generate and fix comprehensive stakeholder consensus on how the functional and institutional core of the internet governance mechanisms should be updated and improved in order to remedy the recently revealed drawbacks and resolve major controversies in this field. However, the Outcome Multistakeholder Statement of the meeting rather marked the start of the process than its fruitful end, and passed the initiative to other formats and coming meetings such as the annual Internet Governance Forum (IGF) and the World Summit on the Information Society +10 (to be conducted at the end of 2015). Still, the IGF 2014, which took place in Istanbul, Turkey on September 2–5, did not show considerable progress in producing a consensus-based multistakeholder vision of the updated institutional design of global internet governance.

Finally, another milestone directly related to the ICT agenda in the BRICS framework was the 6th BRICS summit in Fortaleza, Brazil, which took place on July 15–16, 2014. Unlike at previous summits, this time the ICT issues—though mostly related to information security rather than to internet governance—became one of the major issues for discussion.

For the first time BRICS leaders addressed the Snowden case in a concerted effort by “strongly condemning acts of mass electronic surveillance and data collection of individuals all over the world, as well as violation of the sovereignty of States and of human rights, in particular the right to privacy.” The Fortaleza document also stresses the importance of universally accepted norms and principles of international law for the use of the ICTs, and proposes elaboration of a legally binding instrument for combating transborder cybercrime. The Declaration stresses the need “to preserve ICTs, particularly the Internet, as an instrument of peace and development and to prevent its use as a weapon.” One more important message in the document is the focus of the BRICS states on addressing the common security challenges in the use of ICTs—and elaboration of the idea of a BRICS agreement on cooperation in this field, under the Russian initiative.

Concerning the internet governance issues, the Fortaleza declaration contains no direct support of the format and the outcomes of the NETmundial Meeting. In this regard, the document again translates the position of Russia, which has been persistently criticizing the NETmundial format and disapproved of the Outcome Multistakeholder Statement.

Another interesting moment to mention is that this year the call for a considerable increase in the role of BRICS in the field of internet governance was heard from the international expert community. Just before the summit in Fortaleza, the Just Net Coalition—the international
association of think tanks in the field of internet governance—urged the BRICS states “to provide leadership to the world towards a reform of the U.S. dominated Internet governance structures.” The voices of experts from the United States, Switzerland, France, and many other states that represent the Just Net Coalition (JNC) prove that the demand for a strengthened role for BRICS in this field exists not only within its member-states’ borders.

FIVE STEPS TOWARDS A STRENGTHENED ROLE IN GLOBAL INTERNET GOVERNANCE

What is the potential stake and window of opportunity for BRICS states in this setup, after the Fortaleza summit, NETmundial, IGF-2014 and a year before the Ufa Summit and the WSIS +10 Summit?

First, the challenge and unique opportunity to catch the momentum and create a consensus-based vision of the new global internet governance architecture. The agenda for the WSIS+10 Summit—a milestone event, should have been shaped by now, and BRICS has the full potential to raise its voice on behalf of the non-Western world.

Today, one year after the Edward Snowden revelations, everyone has slammed massive governmental e-surveillance—but no one has provided a vision of checks and balances for the international community aimed at limiting and preventing such precedents in the future. No one has been able to formulate a global Marco Civil—a Set of Principles of Internet Governance, fixing some truly important things. Those might include: (1) limits to governmental e-surveillance and responsibility of states for conducting it; (2) the right of access to the internet; (3) globalization of internet governance, implying responsible international and multistakeholder control over the internet’s critical functions (the IANA 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 regarded as a milestone document summarizing the updated vision of all stakeholders and reflecting the major changes in this area since the adoption of the Okinawa Charter on the Global Information Society of 2000. However, unlike the Okinawa Charter, it should be perceived as a next and unprecedented step in this field—a codification of the principles of internet governance that could be adopted in the form of the UN Convention or a Treaty. Thus, the idea is to negotiate and state the core principles of global stakeholder interaction in the form of a legally binding act—which is a great distance from the declarative status of the Okinawa Charter. At the same time, being just a list of key principles, the document might be regarded as a loose analogue of the Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies adopted on December 19, 1966. The idea is the same—the document does not fix any liabilities of particular parties, but rather postulates the universal principles of cooperation.

However, effective engagement of the global community in the work on such a document requires a strengthened institutionalized global and multistakeholder framework for global internet governance. In particular, the mechanism and mandate of the Internet Governance Forum (IGF) might be developed and transformed in order to establish a permanent IGF Executive Secretariat that would work on a multistakeholder basis under UN auspices on the key goals and issues of the global internet governance agenda. The 9th IGF was conducted in Istanbul on September 2–5, 2014 and the it was marked by calls to strengthen its format and its contribution to global internet governance transformation.

Of course, BRICS states cannot and should not be the only initiators and conveyers of this process since it is obviously a global initiative that requires a contribution from all stakeholders and all regions. However, the BRICS leaders might take the lead in this process in order to make it more oriented towards the developing world and to stress the changes in the global composition of stakeholders towards the non-Western faction.

The BRICS states could not only provide diplomatic support for this initiative and promote it internationally (including at the next IGF and the next BRICS Summit), but also take a leading role in technical and administrative work on establishment of the Executive Secretariat. Moreover, they might take the initiative of hosting this Secretariat—e.g. in Brazil, South Africa,
or Russia, which might be a proper reflection of the rising powers’ increasing role in ICT and the internet governance agenda.

Second the next big issue is determination of the roots and reasons behind the massive governmental surveillance on the internet. Revelations made by Edward Snowden in 2013 made the global technical internet community and policy-makers face a fundamental question: Is systemic and global governmental surveillance of the Net a bug, or a feature of the existing global internet governance model? The answer might imply very concrete and far-reaching consequences on the technical level.

Acknowledging massive e-surveillance as a direct consequence of systemic malfunction of the internet architecture in its present form might imply far-reaching consequences for the technical layer. Besides policy-makers and the issues of trust in international relations, this conclusion might trigger significant revision and update of the technical backbones of the internet. This includes the work of basic internet protocols (HTTP, TCP/IP) and traffic encryption standards. Such ideas have already been announced at the meeting of the Internet Engineering Task Force (IETF) that took place in November 2013 in Vancouver, Canada.

To take the lead in this investigative effort, the BRICS states could facilitate the establishment and work of a Research Committee on Fundamental Risks of the Internet Governance Architecture in the framework of the IGF Executive Secretariat—or within some other UN-based multistakeholder framework. The work of the Committee should be aimed at production and discussion of a Report with recommendations to international policy-makers and the global technical internet community (Internet Society [ISOC], IETF, Internet Architecture Board [IAB], regional Registries, etc.).

However, third, the most thorough investigation of the reasons behind the massive e-surveillance would be fruitless if its conclusions were not used for the creation of mechanisms undermining the incentives for such behavior on the international level. What could BRICS do here, since no law or Set of Principles is able to make the NSA and similar structures in many other countries quit their activities? Building the “confidence matrix” in the field of the use of ICTs might be a strategically wise move. This is just what Russia did on the bilateral level, striking a set of three agreements on CBMs in the cybersecurity area with the United States on June 17, 2013, despite its tensions with Washington on security issues and even despite the following outbreak of the Snowden scandal. Intensive cooperation of national Cyber Emergency Response Teams (CERTs), control of potential cyber-conflict escalation with the help of urgent high-level communication hotlinks, and exchange of data between national Nuclear Risk Reduction Centers turned out to be a good basis for mutual trust building even between the two difficult partners. Half a year later similar mechanisms were adopted for the OSCE, and ASEAN is now on the way to similar CBMs.

BRICS could also make use of the CBM instruments even despite the obvious lack of trust between some of its members (China–India etc.). In addition to sharing information on major abnormalities of transborder traffic and cybersecurity incidents, parties to the CBMs agreements could join forces to monitor cyber espionage and e-surveillance campaigns targeted at their territory and infrastructure by third parties. Here all BRICS countries have a common stake, and the diversity of their cyber infrastructure in terms of geography and technology could enable a synergy in locating e-surveillance activities and tracking their source. As a further step, BRICS states might think of enabling greater openness of their own transborder flow for their partners in the forum in order to show that they do not conduct cyber espionage or surveillance activities themselves. The idea of CBMs in the field of use of ICTs should be in demand for most countries in the forum. One potential proponent is Brazil, where President Dilma Rousseff and the biggest national oil company PetroBras became victims of NSA e-surveillance programs.

Another potential advocate of this approach is Russia—first, because it successfully tested the format of CBMs in the information security area and is willing to foster its further development in multilateral and bilateral frameworks. However, Russia is widely known as a consistent architect of the global regime of cyber-governance aimed at prevention of the use of cyber-weapons and “digital disarmament.” Therefore, the CBM mechanism implemented in the BRICS framework might be a good tool for responding to a number of information security issues. One example is leveraging cooperation of CERTs (or creating BRICS-CERT
or BRICS-CSIRT) as a part of CBMs, which would also help to counter transborder cybercrime and cyber terrorism.

In fact, the whole CBM arsenal can be regarded as complementary to the mechanism of real-time 24/7 transborder information exchange on cybercrime and other cybersecurity incidents. Of course, this demands the level of trust that is not always present currently among BRICS states—but if the countries start with small but effective cooperation (defending themselves together against third parties’ activities) a positive result will likely be just a matter of time. Finally, the BRICS-based CBM network in the case of its successful operation might involve new members, thus becoming a core for a wider international “trust network” and raising its synergy effects. This would be a good basis for a new global mechanism for fighting cybercrime and cyber terrorism that has been promoted by Russia and some of its allies (e.g. the idea of a global universal UN Convention on countering transborder cybercrime).

Fourth, one more essential component of the ICT agenda as a potential pillar of BRICS activities is joint IT-infrastructure and internet-sector projects. These should be large in order to stimulate policy-level debates and to correspond to the size of the forum’s economies. They also should be global or transregional in order to keep all BRICS states interested and engaged.

For the moment, members of the forum have already accumulated enough experience, technological background, financial resources, and political leadership to move this agenda forward in a more dynamic way. The first project of its kind was probably the BRICS Internet Cable, aimed at diversification of the global network of backbone transcontinental fiber-optic cables. However, the project of the 32,000km cable connecting Russian Vladivostok with Brazilian Fortaleza through Indian and Chinese hubs has not been finished yet though its implementation was initially scheduled for 2012–2013. However, once it is finished, what are the next steps?

The probable answer includes major software development initiatives that might bring together market demands and certain policy imperatives for the BRICS states. Therefore, the BRICS states could join their human, financial, and technological resources to develop better security standards for the Internet protocols, protected operation systems, and applications. Strangely, detailed recommendations on this issue were already provided specially to BRICS by the Just Net Coalition (JNC)—a “global network of civil society actors committed to an open, free, just and equitable Internet,” established in February 2014 and bringing together both Western experts and representatives of the developing world including many Indian experts. In the Statement to the BRICS Summit in Fortaleza, the JNC experts identified four possible areas of synergies for BRICS states in the ICT field. One of them was “the development of new open Internet platforms and tools including in the areas like search, operating systems, data storage and cloud services given that they have the necessary skills, large internal markets and political motivation to break with the current mass surveillance and rent-seeking based business models.” It should be noted that this list mostly follows in line with the priorities of the “digital sovereignty” concept that is often mentioned in Russia and in many other states today. Looping the issue back to e-surveillance, those joint activities might also include elaboration of not only protected internet protocols, but also new cryptography standards and products, including market-oriented solutions for “civil cryptography.” The BRICS-led effort might serve as an incentive for innovations on a nationwide level, e.g. for the Russian ICT cryptography market and its regulation.

Fifth and finally, the BRICS states could increase and strengthen their cooperation with technical organizations in the global internet community. One particular goal of such cooperation might include launching training and educational programs on legal, technical, and political aspects of internet governance. Such activities should not only be supported with money and expertise, but also incorporated into the academic schedules of state universities and other institutions of higher education in Russia, China, Brazil, etc. In a longer-term prospect, this will contribute to greater participation and a louder voice of BRICS
experts in the work of IETF, ISOC, IAB, regional internet registries (RIRs), and other organizations shaping the future of the Net on technological level.

One specific direction of collaboration with the technical community might include building connections between BRICS and ICANN. In fact, the process has already started among the BRICS countries on a bilateral level: the first steps were made with the decision to hold the NETmundial Global Meeting in São Paulo, Brazil. Before that, ICANN launched a dialogue on strategic cooperation with China and opened its regional office in Beijing in 2012. In February 2014, ICANN CEO Fadi Chehade made a three-day visit to China and held negotiations with three Chinese Ministers with the aim of further development of this strategic dialogue and cooperation. Russia now looks like a potential next link in this chain of emerging cooperation between ICANN and BRICS states, as well as India. The benefits of the dialogue with ICANN now include the opportunity to promote BRICS interests and vision concerning the IANA oversight transition to the global stakeholder community, to leverage educational and training efforts in the field of internet governance, and to promote the development and expansion of top-level domain name spaces (including .BRICS?).

***

Neither of these projects and initiatives should be regarded as a silver bullet for the challenges the BRICS countries face in the ICT area. Equally, the ICT agenda itself is not a silver bullet for the forum’s questionable identity or relatively low practical output of its initiatives. And yet it totally meets the fundamental goal of the BRICS format—to facilitate transformation of the global governance architecture in a way that corresponds with the interests and needs of the global community including the non-Western world. Besides, the transborder nature of the Internet makes the BRICS format free of its most serious weaknesses such as a clash of regional interests and mismatch of geographically determined agendas. Instead, the Internet brings BRICS states and its stakeholders together. This is why the goal of installing the ICT agenda as another pillar of BRICS identity is a worthy goal before the forum’s 2015 Summit in Ufa, Russia.

NOTES


3 Ibid., Paragraph 50.

4 Ibid., Paragraph 49.


Twenty years ago the issue of nuclear weapons on Ukraine's territory, and of security assurances to be given to Ukraine in return for becoming a non-nuclear-weapon state, was at the center of attention of politicians, diplomats, and the international expert community. It seemed at the time that the problem had been resolved once and for all: first in the Triilateral Statement by the Russian, U.S., and Ukrainian presidents (Moscow, January 14, 1994), and then in the Budapest Memorandum on Security Assurances in connection with Ukraine's accession to the Nuclear Non-Proliferation Treaty (Budapest, December 5, 1994), signed by Russia, the UK, and the United States.

However, in spring 2014 when the Crimean crisis broke out, the question came into Russian and international and policy discourse as to whether the Budapest Memorandum was still in force.

Each of the possible answers provoked further questions: if the Budapest Memorandum should still have been considered as a valid and acting mechanism, what are the implications for European and global security in the event of further escalation? The question turned out to be from idle curiosity since a few months later we witnessed the escalation of the crisis in the Eastern Ukraine.

On the other hand, denying the relevance of the Budapest Memorandum in the new conditions of the crisis in Crimea would have inevitably raised the issue of the implications for Ukraine, Crimea, and each of the three states that gave Ukraine security assurances.

The more so as from 1991 I was closely involved in the discussions on the USSR's nuclear legacy, including, first and foremost, the question of soviet nuclear weapons in Ukraine. On December 1, 1991, I bitterly watched in Kiev as the final chord for the Soviet breakup was struck during the Ukrainian independence referendum, which, rather than the subsequent Belavezha accords, marked a coup de grace to the Soviet Union. on September 3, 1993, in Massandra (Crimea), together with Boris Yeltsin and Russian negotiators, I witnessed the Ukrainians essentially thwart all bilateral decisions on nuclear weapons in anticipation of Washington's joining the negotiations. In January 1994, I was concerned with the analysis of the Triilateral statement and discussed it, first of all, in Kiev, and then, right up to the spring of 1995, I participated in the efforts to bring closer the non-nuclear status of Ukraine as a party to the Treaty on the Non-Proliferation of Nuclear Weapons, the culmination of which was the attendance of the Ukrainian delegation at the 1995 NPT review and extension conference, to which Ukraine came having finally confirmed its non-nuclear status.

On December 22, 1991 Mikhail Gorbachev handed over the nuclear briefcase to Boris Yeltsin. That was part of the answer to the question of who controls the former Soviet Union's strategic nuclear forces.

On December 30, 1991 in Minsk the CIS member states signed an agreement on strategic nuclear forces. The agreement recognized "the necessity for a coordinated and organized solution to issues in the sphere of the control of the strategic forces and the single control
over nuclear weapons...."1 Article IV of the agreement stipulated that "until the complete elimination of nuclear weapons, the decision on the need for their use is taken by the president of the Russian Federation in agreement with the heads of the Republic of Belarus, the Republic of Kazakhstan and the Republic of Ukraine, and in consultation with the heads of the other member-states of the Commonwealth."2

The Agreement further stipulated that "until their destruction in full, nuclear weapons located on the territory of the Republic of Ukraine shall be under the control of the Combined Strategic Forces Command, with the aim that they not be used and be dismantled by the end of 1994." The parties agreed that the disposal of nuclear weapons stationed in Belarus and Ukraine should be conducted "under the joint control of the Commonwealth states." The Agreement would be considered "terminated" in respect of the states that have removed strategic forces and nuclear weapons from their territory.

Nevertheless, the joint strategic forces were never actually set up. The very idea of their creation was probably a compromise, a temporary concession which Russia made at a difficult time immediately after the collapse of the Soviet Union, when Moscow intended to pursue energetic market reforms and needed the understanding of its CIS neighbors. Other reasons for the attempt to establish joint strategic forces included, first, the need to address deep Western concerns, and second, Boris Yeltsin’s wish to ensure a supportive neutrality of the top brass during the dismantlement of the Soviet Union (one of the demands of the Soviet military leadership at the time was that a united command of the nuclear arsenal be preserved).

An in-depth look at the agreement on the joint strategic forces suggests that its key clauses required further clarification—especially those dealing with the practical mechanisms of control over the nuclear button, the modalities of making decisions if the need ever arose to authorize the use of nuclear weapons, and the financing of the strategic nuclear forces. Apart from Russia, none of the former Soviet republics had the capability to ensure proper combat readiness, technical maintenance, and security of nuclear ammunition. Besides, only Russia had the highly skilled personnel required for these tasks, and only Russia could afford to pay the minimally adequate wages to that personnel. In addition, the very idea of several states parties being in control (albeit “joint” control) of nuclear weapons caused grave concerns among the other nuclear-weapon states. They argued that such a situation would increase the unpredictability of the behavior of the Soviet Union’s successor states. “Who controls the nuclear button?”—that was the question politicians and the media all over the world were asking in late 1991 and early 1992.

On July 6, 1992 nine CIS states (Armenia, Belarus, Kazakhstan, Kyrgyzstan, Tajikistan, Uzbekistan, Ukraine, Moldova, and Turkmenistan) reaffirmed their support for Russia’s membership of the NPT as a nuclear-weapon state. They further declared their willingness to join the treaty as non-nuclear-weapon states. That settled the legal issue of succession, and Russia became a fully legitimate successor of the Soviet Union as far as possession of nuclear weapons was concerned. It was agreed that Russia was the rightful owner of the entire Soviet nuclear arsenal, including the weapons stationed in Ukraine, Belarus, and Kazakhstan.

THE MASSANDRA EFFECT

The Ukrainian government had also declared its willingness to relinquish the nuclear weapons stationed on its territory. In practice, however, it was doing all it could to delay the resolution of various issues related to the elimination of those weapons, thereby raising questions as to whether nuclear warheads on its territory really belonged to Russia. Ukraine also voiced the notion that even though Russia had operational control of strategic nuclear weapons stationed on Ukrainian territory, the actual title to the warheads as well as the delivery systems belonged to Kiev.

On May 23, 1992 the United States, Russia, Ukraine, Belarus, and Kazakhstan signed the Lisbon Protocol to the Strategic Arms Reduction Treaty (START I) between the Soviet Union and the United States. Under that protocol, Ukraine, Belarus, and Kazakhstan were recognized as state parties to START I, along with Russia. They undertook the obligation to eliminate all strategic nuclear warheads or to remove them to Russia once the treaty had entered into force.
Belarus and Kazakhstan duly fulfilled all their commitments under the Lisbon Protocol. At the same time, the issue of the nuclear warheads and delivery systems stationed in Ukraine proved extremely difficult. In fact, it took another three years to resolve this issue.

When the Soviet Union broke up, the strategic nuclear forces stationed in Ukraine included 130 SS-19 intercontinental ballistic missiles (ICBM) carrying 780 warheads, and 46 SS-24 ICBMs carrying 460 warheads, plus about 600 warheads that used Tu-95 MS and Tu-160 heavy bombers as delivery systems. This meant that the nuclear arsenal stationed on Ukrainian territory was bigger than the arsenals of Britain, France, and China put together. The Ukrainian government and parliament had declared on more than one occasion that the elimination of nuclear weapons stationed in Ukraine was one of their main foreign-policy priorities. In practice, however, Ukraine's conduct belied its words. Kiev was making deliberate efforts to acquire the status of rightful owner of the strategic nuclear weapons stationed in Ukraine. When Russia, Ukraine, Belarus, and Kazakhstan signed the documents on the succession under the START I treaty, the heads of state—including Ukrainian president Leonid Kravchuk—simultaneously sent letters to the U.S. president pledging to eliminate nuclear weapons on their territory and join the NPT. But Ukrainian officials soon declared that the letter was nothing more than a "personal message that is not legally binding."

On September 3, 1993, at a meeting in Massandra, Crimea, Russian Prime Minister Viktor Chernomyrdin and his Ukrainian counterpart Leonid Kuchma signed three protocols: on guarantees of supervision over missile launchers, on the disposal of nuclear ammunition, and on key principles of the disposal of nuclear warheads. Under these agreements, the entire nuclear arsenal stationed in Ukraine was to be removed to Russia and dismantled at the facilities where those warheads were made. Under a protocol signed in Massandra, highly enriched uranium (HEU) extracted from nuclear warheads was to be diluted to low-enriched uranium and then returned to Ukraine for use as nuclear energy reactor fuel.

But then came a completely unexpected twist, which I personally witnessed, and which had very little to do with normal diplomatic practice. The Ukrainian delegation made hand-written changes to the documents already signed; these changes completely altered the essence of the agreement. In effect, Ukraine agreed to dismantle and remove to Russia only the warheads fitted on the SS-19 missiles. In accordance with the hand-written amendment, the SS-24 missiles could remain on Ukrainian territory. A member of the Russian delegation at the talks with Ukraine described that stunt as "completely unprecedented in diplomatic practice," and Russia denounced the agreement.

Serhiy Holovaty, a prominent Ukrainian politician (who has served as a member of the Ukrainian parliament and then as a justice minister) offered me the following ostensible explanation at the time: "We need to have a strong deterrent against Russia's aggressive policies. Otherwise Ukraine will share the fate that has already befallen Georgia, Moldova, and Tajikistan, where Russia is using imperial methods in pursuit of its vital interests."

Ukraine's real motive, I believe, was quite different. The country's genuine security interests took second stage to its economic interests. Ukraine was in the throes of a severe economic crisis, so Kiev was merely haggling to secure as much financial assistance as it could from the United States. The same opinion was unequivocally voiced by U.S. ambassador at large James Goodby, who led negotiations with Ukraine in 1992–1994. It is also obvious that Ukraine was trying to extract large sums of money or some financial concessions from Russia, especially by way of compensation for the HEU contained in the nuclear warheads.

In 1992–1993 Ukraine lacked the capability to establish independent and effective operational control over all the warheads remaining on its territory (in other words, it could neither launch those warheads nor prevent their launch). At the same time, it was capable of establishing partial control over nuclear warheads after a period estimated to be from several months to one and half years. In essence, there was only a possibility of Ukraine establishing negative control, i.e. being able to prevent the launch of missiles from its territory unless the government in Kiev had given its consent for that launch. As for positive control, experts offered different opinions. The prevailing view was that not all the possibilities for Ukraine establishing positive control over missiles on its territory had been cut off. First, the decoders (electronic locks) used in Soviet nuclear weapons were made in Kharkiv, Ukraine. Second, the command station of the 46th Missile Army, which controlled all communication lines to
the local command stations and missile launchers, was situated in Vinnytsya, Ukraine. Third, the Ukrainian military had the theoretical capability to calculate missile trajectories, and therefore to program the mission input data for ICBMs.

At the same time, Ukraine lacked access to the satellite data required for precise programming of new ICBM targets. As a result, Kiev’s real ability to establish positive control was minimal or even nonexistent. Finally, Ukraine’s financial and economic situation in 1992–1993 would have prevented any attempts to relocate the missiles to new bases (which the Ukrainian military-political leadership was unlikely to contemplate in the first place), let alone to establish effective positive control over the nuclear arsenal.

Meanwhile, serious questions remained in 1992 and 1993 over Ukraine’s ability and willingness to act as a responsible state party to international treaties.

**MASTERS OF NUCLEAR BLUFF**

Ukraine’s nuclear policy in 1992–1993 essentially amounted to nuclear bluff. The purpose of that bluff was, first, to increase the newly independent republic’s international prestige and, second, to secure substantial Western economic assistance in return for subsequent removal to Russia of the warheads stationed on Ukrainian territory. That was the whole purpose of the Ukrainian parliament’s resolution adopted in November 1993; to all intents and purposes, the document declared that Ukraine was a nuclear-weapon state.

It is also worth noting that even though Russian diplomats and generals were engaged in energetic negotiations with their Ukrainian counterparts, the Massandra Effect continued to plague most of these discussions. The positions of the two sides seemed very close, but a comprehensive agreement always seemed just out of reach. The explanation was simple: Kiev knew very well that the key to the safe with hard currency was in Washington, not Moscow. Besides, Ukrainian negotiators believed that Washington was far more interested than Moscow in ensuring the success of the 1995 NPT Review Conference and securing the decision to extend the NPT indefinitely. Kiev rightly believed that if Ukraine were to refuse to take part in the conference as a non-nuclear-weapon state, the whole conference would be overshadowed by such a decision. It would throw a spanner in the entire effort to achieve the desired outcome of the conference, and set an example of ignoring the NPT for other states.

As a result, negotiating an effective agreement on the future of the Russian nuclear warheads stationed in Ukraine without the involvement of the United States was proving impossible. Russia was initially confident that, one way or another, the problem would be resolved bilaterally, in a “fraternal” manner, and without the involvement of third parties. In the end, however, it was forced to admit its inability to achieve the result without the United States, with Washington not merely acting as a symbolic mediator but actually playing a crucial, if not leading role.

**THE TRILATERAL STATEMENT**

It must be admitted that, on the whole, Ukraine’s strategy had achieved its goal. On January 14, 1994 the presidents of Russia, Ukraine, and the United States signed the Trilateral Statement under which Ukraine undertook to have all nuclear warheads removed from its territory within seven years from the START I treaty entering into force.

Just as the Ukrainian leadership had insisted all along, the Trilateral Statement was directly linked to the provision of 125 million dollars in aid by the United States, as well as compensation in the form of low-enriched uranium (LEU). That assistance package was later increased even further.

Ukraine’s paramount goal at the talks was to secure some economic gains in return for relinquishing the nuclear weapons that remained on its territory, even though Kiev had no control over those weapons.

Viewed from today’s perspective, the crucial turn probably came when presidents Yeltsin and Clinton agreed to give Ukraine security assurances. Both told their Ukrainian counterpart
Leonid Kravchuk that as soon as the START I treaty entered into force and Ukraine became a non-nuclear weapon state party to the NPT, Russia and the United States would:

- Reaffirm their commitment to Ukraine, in accordance with the principles of the CSCE Final Act, to respect the independence and sovereignty and the existing borders of the CSCE member states and recognize that border changes can be made only by peaceful and consensual means; and reaffirm their obligation to refrain from the threat or use of force against the territorial integrity or political independence of any state, and that none of their weapons will ever be used except in self-defense or otherwise in accordance with the Charter of the United Nations;

- Reaffirm their commitment to Ukraine, in accordance with the principles of the CSCE Final Act, to refrain from economic coercion designed to subordinate to their own interest the exercise by another CSCE participating state of the rights inherent in its sovereignty and thus to secure advantages of any kind;

- Reaffirm their commitment to seek immediate UN Security Council action to provide assistance to Ukraine, as a non-nuclear-weapon state party to the NPT, if Ukraine should become a victim of an act of aggression or an object of a threat of aggression in which nuclear weapons are used;

- Reaffirm, in the case of Ukraine, their commitment not to use nuclear weapons against any non-nuclear-weapon state party to the NPT, except in the case of an attack on themselves, their territories or dependent territories, their armed forces, or their allies, by such a state in association or alliance with a nuclear weapon state."

Yeltsin and Clinton also informed Kravchuk that they had held consultations with the UK, the third NPT depository state, and that London was also ready to give the same security assurances to Kiev as soon as Ukraine became a non-nuclear-weapon state party to the NPT.

THE BUDAPEST MEMORANDUM

It appeared that Ukraine had achieved everything it wanted. Still, even after the signing of the document the Ukrainian parliament was in no rush to ratify the NPT. In the run-up to the 1995 NPT Review Conference, such delays were especially worrying for U.S. diplomats. They thought it was necessary to ensure Ukraine’s participation in that conference as a full member of the NPT, thereby demonstrating the success achieved by the nuclear-weapon states (especially the United States) in overcoming the potential threats posed by the break-up of the Soviet Union.

Meanwhile, the nature of American pressure on Ukraine underwent a significant transformation: from sticks in 1992 to numerous carrots in 1993 and 1994. Also, Washington’s pressure on Ukraine on the issue of nuclear weapons contrasted sharply with the Russian position during the same period. Moscow was engaged in grueling talks with Ukrainian delegations, but Russian negotiators often seemed lethargic, and clearly lacked initiative. Neither were they very forceful in seeking Ukraine’s compliance with the agreements that had already been achieved.

Nevertheless, by the autumn of 1994 the Ukrainian parliament started to feel rapidly mounting international pressure (especially by the United States). By that time the Ukrainian leadership had already concluded beyond any doubt that it would be impossible for the country to maintain a nuclear arsenal, and that it would be preferable to abide by the terms of the Trilateral Statement. Any further delays in Ukrainian ratification of the NPT as a non-nuclear weapon state, especially in the run-up to the final, decisive sitting of the NPT Conference Preparatory Committee (PrepCom), posed the risk of Ukraine’s international isolation. Having realized that the opportunity for nuclear bluff or nuclear haggling had been exhausted, on November 16, 1994 the Ukrainian parliament ratified the NPT by 301 votes to 8 in the 450-seat chamber. But it made the ratification conditional on the nuclear-weapon states giving Ukraine special security assurances. Three NPT depository states—the United States, Russia, and the UK—issued such guarantees in a joint memorandum at the Conference on Security and Cooperation in Europe (Budapest, December 5, 1994). France and China approved separate documents that also gave Ukraine security assurances.
The first five paragraphs of the Budapest Memorandum repeat the Trilateral Statement, for the most part. But there are also some differences in the text, so I will cite these five paragraphs here:

1. "The United States of America, the Russian Federation, and the United Kingdom of Great Britain and Northern Ireland, reaffirm their commitment to Ukraine, in accordance with the principles of the CSCE Final Act, to respect the Independence and Sovereignty and the existing borders of Ukraine.

2. The United States of America, the Russian Federation, and the United Kingdom of Great Britain and Northern Ireland, reaffirm their obligation to refrain from the threat or use of force against the territorial integrity or political independence of Ukraine, and that none of their weapons will ever be used against Ukraine except in self-defense or otherwise in accordance with the Charter of the United Nations.

3. The United States of America, the Russian Federation, and the United Kingdom of Great Britain and Northern Ireland, reaffirm their commitment to Ukraine, in accordance with the principles of the CSCE Final Act, to refrain from economic coercion designed to subordinate to their own interest the exercise by Ukraine of the rights inherent in its sovereignty and thus to secure advantages of any kind.

4. The United States of America, the Russian Federation, and the United Kingdom of Great Britain and Northern Ireland, reaffirm their commitment to seek immediate United Nations Security Council action to provide assistance to Ukraine, as a non-nuclear-weapon State Party to the Treaty on the Non-Proliferation of Nuclear Weapons, if Ukraine should become a victim of an act of aggression or an object of a threat of aggression in which nuclear weapons are used.

5. The United States of America, the Russian Federation, and the United Kingdom of Great Britain and Northern Ireland, reaffirm, in the case of the Ukraine, their commitment not to use nuclear weapons against any non-nuclear-weapon State Party to the Treaty on the Non-Proliferation of Nuclear Weapons, except in the case of an attack on themselves, their territories or dependent territories, their armed forces, or their allies, by such a state in association or alliance with a nuclear weapon state."

Compared with the Trilateral Statement, Paragraph 1 of the Budapest Memorandum does not contain the words "and recognize that border changes can be made only by peaceful and consensual means." In other words, the Budapest Memorandum seems to rule out the very possibility of a revision of borders, and omits the term "consensual means."

After numerous delays, Ukraine finally joined the NPT on December 5, 1994. From the legal point of view, that step eliminated a significant source of tension and a potential source of nuclear proliferation on former Soviet territory. Another important factor is that Ukraine’s accession to the NPT as a non-nuclear-weapon state enabled the entry into force of the START I treaty, which was originally signed by the Soviet Union and the United States, and which Russia, Ukraine, Belarus, and Kazakhstan later joined under the Lisbon Protocol. The Russian parliament had ratified START I with a reservation that the treaty would enter into force in Russia only once Ukraine had joined the NPT.

From then on Ukraine diligently implemented all its commitments under the Trilateral Statement and the START I treaty (with the Lisbon Protocol). The last nuclear warhead was removed from Ukrainian territory to Russia in June 1996.

SECURITY ASSURANCES IN THE POST-CRIMEA ERA

The entire saga of Ukraine formalizing its non-nuclear-weapon status in 1991–1994 demonstrates that Russia’s ability to influence even its own CIS neighbors was extremely limited at the time. In truth, until the United States joined the Russian–Ukrainian agreements in January 1994, those agreements were not being honored.

It must be recognized that, had the United States not become involved, Ukraine probably would not have agreed to a full elimination of nuclear weapons stationed on its territory, or it would have dragged its feet on that matter for an unacceptably long time. The United States had essentially demonstrated during that period that it was holding the keys to the Kiev offices where the main political decisions were being made.

138 SECURITY ASSURANCES TO UKRAINE AND THE 1994 BUDAPEST MEMORANDUM
Another conclusion that can be made from the events of 20 years ago is that Ukraine was acting inconsistently and sometimes dishonestly at the negotiations with Russia. Those who believe that such Ukrainian tactics are a fairly recent phenomenon, or the result of anti-Russian views held by some individual Ukrainian politicians, are quite wrong. Ukraine has swindled Russia on some extremely important international issues on more than one occasion.

The Trilateral Statement and the Budapest Memorandum were adopted in another historical era; that era was gone in spring 2014. As Dmitry Trenin, head of the Carnegie Moscow Center, put it at a meeting of Triadogue Club International on March 5, 2014, it was a short era sandwiched between two cold wars. During that era, Russia was severely weakened militarily, financially, and economically. As a result, the scope for Russian diplomacy was greatly restricted.

The fact that it was a bygone historical era is also demonstrated by some other quotes from the Trilateral Statement. For example, the statement contains a prominent reference to the START II treaty: “Presidents Clinton and Yeltsin noted that entry into force of START I will allow them to seek early ratification of START II. The Presidents discussed, in this regard, steps their countries would take to resolve certain nuclear weapons question.” As we all know, the START II treaty was never ratified by the United States, even though the Russian parliament did ratify it.

As a result, those members of the new Russian elite who study the Trilateral Statement and the Budapest Memorandum of 20 years ago have a distinct feeling that Washington was cherry picking the elements it wanted, and conveniently forgetting about the parts in which Russia had an interest.

Another indication that the documents were signed in a bygone historical era is the fact that Washington’s commitment in the Trilateral Statement to “respect the independence and sovereignty and the existing borders of the CSCE member states” (all CSCE states, and not just Ukraine!) did not later prevent it from facilitating Kosovo’s secession from Serbia and then recognizing Kosovo as an independent state.

Back on March 4, 2014, at the beginning of the Crimean crisis, before the events in the Donbass region, President Putin left the question of the Budapest Memorandum open and largely dependent on the position of the United States and Great Britain regarding the (non) recognition of the new government in Kiev.

In fact it was assumed that if Washington and London had recognized that the events that happened in Kiev in February were a coup d’État, then the Budapest Memorandum might have remained in force, and the three parties (Russia, the United States, and the UK) should work together on restoring the legitimacy of the government in Kiev.

However, the situation would have been entirely different if the United States and the UK had claimed that the events in Kiev were a revolution. Then, in March 2014, Putin asked: “What does that mean? In such a case, it is hard for me to disagree with those of our experts who argue that a new state has emerged on [Ukrainian] territory, in the same way that a new state emerged after the 1917 revolution and the collapse of the Russian Empire. And we have not signed any binding documents with that new state, or with regard to that state.” In other words, for the Kremlin the Budapest Memorandum became more dead than alive, from the moment when Washington and London both recognized the legitimacy of the new government in Kiev.

As we observe the recent past of the Crimean crisis today, it is of little doubt that after half a year of events developing at a breathtaking pace the question of whether the Budapest Memorandum still remains in force de jure has almost disappeared from the agenda. In this new era, whatever developments we witness around the Crimea and Ukraine in the future, the issue of 20-year-old security assurances has largely moved to the domain of academic discussions.

NOTES

1 “Agreement between States—Parties to the Commonwealth of Independent States on Strategic Forces. Minsk, December 30, 1991,” information newsletter of the Council of

2 Ibid.


Demidov, Oleg is the Director of the Program “International Information Security and Global Internet Governance” at PIR Center and a Ph.D student at the Faculty of Political Science at Moscow State Institute of International Relations (MGIMO-University). In 2011–2012 held the position of Project Coordinator at Center for Political and International Studies (CPIS) under the International Federation for Peace and Conciliation. From 2012 has been an expert at the Commission on Information Security and Cybercrime in the Russian Association for Electronic Communications (RAEC). From 2013 has been the member of the Research Advisory Network (RAN) under the Global Commission on Internet Governance (GCIG). E-mail address: demidov@pircenter.org.

Evans, David is the Senior Director and Chief Technologist at Cisco Internet Business Solutions Group (IBSG) Innovations Practice. From August 1990 to May 2014 served as the Chief Futurist for Cisco. Previously a member of the Corporate Technology Group (CTG); was responsible for identifying disruptive technologies that were relevant and aligned to Cisco. An expert on emerging technologies, holds numerous patents in the fields of connected car, RFID, virtual people, mobile phone technology. The field of professional interests includes
topics such as the Internet of Everything (IoE) and The Net Effect, as well as the technological phenomena of Big Data, Augmented Reality, 3D printing as well as their social and economic implications on a global scale. Shared his views on these issues in Forbes, Fortune, CNN, San Jose Mercury News, New York Times, Nikkei, MSNBC, Discovery Channel, History Channel, as well as numerous other media outlets.

**Fedorov, Yuri, Dr.**, is an Associate Fellow in the Chatham House – The Royal Institute of International Affairs (London, UK). Security Index Editorial Board member. Graduated from the Moscow State University’s Physics Department. Worked at the Sociological Research Institute of the USSR Academy of Sciences, and headed the section on disarmament issues at the Institute for International Economy and International Relations (IMEGO) RAS. Also worked in the international division of the Soviet Communist Party Central Committee, after which, in 1991, took the post of Deputy Head of the political science department at MGIMO. In 1998 became section head, and in 2000 head of the division on military policy research at the U.S. and Canada Institute RAS. In 2001–2002 served as the PIR Center Deputy Director. In 2002–2003 was Deputy Director of the Institute of Applied International Research. Author of a monograph entitled “Substrategic Nuclear Weapons and Russian Security Interests” (2001). E-mail address: fedorov.yury@yahoo.com.

**Ibragimova, Galiya, Dr.,** is PIR Center Consultant, the Coordinator of the iSi (International Security Index) Project. Post-graduate student of the University of World Economy and Diplomacy (Tashkent, Uzbekistan). Graduated from the University of World Economy and Diplomacy. In 2008–2009 participated in Professional Management Program (intensive MBA program) at the Uzbekistan-Japan Center for Human Development. Has the Project Management Professional (PMP) degree. Graduate of the PIR Center International Summer School on Global Security. PIR Center intern in 2009. Research interests include the issues of regional security in Central Asia, and information security. E-mail address: ibragimova@pircenter.org.

**Kalinina, Natalia, Dr., Prof.**, is a Senior Research Fellow, Head of the group on unconventional threats to security in the Center for International Security Studies at the Institute of World Economy and International Relations (IMEGO), Russia Academy of Sciences. One of the leading experts in the field of chemical and biological disarmament. Experienced scientist, auditor, multilateral person, whose researches in biologics, chemistry, policy, economy are of invaluable contribution to the science and for further research perspectives. From 1994 to 2007 worked for central organs of political departments of the Russian Federation, including the post of Assistant to the Chairman of the Government of the Russian Federation in 2003–2004. and Deputy head of the inspection of the Accounts Chamber of the Russian Federation in 2005–2007. PIR Center Advisory Board member. E-mail address: kalinina@imego.ru.

**Kovchegin, Dmitry** is an independent researcher on the issues of nuclear safety. Previously worked as the Project Consultant for the Russian-US program of cooperation in improving the security, accounting and controls at Russian Nuclear facilities, also worked for the Moscow office of Booz Allen Hamilton Inc. Served as a Research Fellow at PIR Center and the Belfer center for Science and International Affairs at Harvard University. Graduate of the Moscow Engineering and Physics Institute program on security, accounting and controls of nuclear materials and nonproliferation. Member of the Working Group on International Cooperation in Nonproliferation and Nuclear Security under the PIR Center’s Advisory Board since 2012. E-mail address: kovchegin@yahoo.com.

**Orlov, Vladimir, Dr.,** is the founder and the President of the PIR Center and the Editor-in-Chief of the Security Index journal. Graduated from the Moscow State Institute of International Affairs (MGIMO). Member of the Public Board at the Ministry of Defense of the Russian Federation, a member of the Russian Pugwash Committee under the Presidium of the Russian Academy of Sciences, a member of the Russian National Committee for BRICS Studies Research Council, a member of the Monterey Non-Proliferation Strategy Group, a member of the International Nuclear Energy Academy (INEA), a member and the founder (1993) of the Triadogue Club International, and member of the Washington Quarterly Editorial Board. Currently serves as the Associate Research Fellow at the Geneva Center for Security Policy (GCSP). In 2001–2002 served as the UN consultant on disarmament and nonproliferation education by appointment of the UN Secretary General. During the 2010 NPT Review Conference served as a member of the official delegation of the Russian Federation. Regularly publishes his views in Russian and foreign periodicals and has edited more than a dozen books on international security issues.
published both in Russia and abroad. Continues to teach on a regular basis, giving lectures on Russian foreign policy and WMD nonproliferation. E-mail address: orlov@pircenter.org.


Skorokhodova, Olga is a Ph.D student in the history and theory of international relations at Moscow State University of Lomonosov, Faculty of History. From October to December 2013 held the position of an Intern at PIR Center and conducted an in-depth study on trade and security cooperation with Myanmar. In 2012–2013 academic year, studied at the MacMillan Center for International and Regional Studies at Yale University Fox International Fellow. Student of the PIR Center’s International Summer School on Global Security of 2013. Research interests embrace the issues of energy politics and security policy in the Greater Middle East and Southeast Asia. Speaks Russian, English, French and Spanish. E-mail address: olga.n.skorokhodova@gmail.com.

Zolotukhin, Ivan, Dr. is the Assistant Professor at the International Affairs Department and the Director of the principle educational program “International Relations” at the Far East Federal University. Member of the Academic Board of the School of Regional and International Studies at the Far East Federal University (DVFU). In 2000 graduated from the Faculty of History at DVFU with a degree in regional studies. Up to 2011 held the post of the Dean of the Faculty of International Relations at the Vladivostok Institute of International Relations under then Far East State University (VIMO DVGU). In 2010 made in the internship in the USA in the framework of the Open World Program, and in 2012 completed the internship at the University of California, Berkeley. The sphere of research interests includes security and policy-making process in the Asia Pacific region, geopolitics, and Russian cooperation with the ASEAN states. E-mail address: zolivnik@mail.ru.
published both in Russia and aboard. Continues to teach on a regular basis, giving lectures on Russian foreign policy and WMD nonproliferation. E-mail address: orlov@pircenter.org.


Skorokhodova, Olga is a Ph.D student in the history and theory of international relations at Moscow State University of Lomonosov, Faculty of History. From October to December 2013 held the position of an Intern at PIR Center and conducted an in-depth study on trade and security cooperation with Myanmar. In 2012–2013 academic year, studied at the MacMillan Center for International and Regional Studies at Yale University Fox International Fellow. Student of the PIR Center’s International Summer School on Global Security of 2013. Research interests embrace the issues of energy politics and security policy in the Greater Middle East and Southeast Asia. Speaks Russian, English, French and Spanish. Email address: olga.n.skorokhodova@gmail.com.

Zolotukhin, Ivan, Dr. is the Assistant Professor at the International Affairs Department and the Director of the principle educational program “International Relations” at the Far East Federal University. Member of the Academic Board of the School of Regional and International Studies at the Far East Federal University (DVFU). In 2000 graduated from the Faculty of History at DVFU with a degree in regional studies. Up to 2011 held the post of the Dean of the Faculty of International Relations at the Vladivostok Institute of International Relations under then Far East State University (VIMO DVGU). In 2010 made in the internship in the USA in the framework of the Open World Program, and in 2012 completed the internship at the University of California, Berkeley. The sphere of research interests includes security and policy-making process in the Asia Pacific region, geopolitics, and Russian cooperation with the ASEAN states. E-mail address: zolivnik@mail.ru.
Alert me

Taylor & Francis Online offers a range of email and RSS alerts to keep you up to date with our publications

To find out more, visit:
www.tandfonline.com/alerting
“What does that awe-inspiring progress of yours foretell? (...) Rent into a thousand shreds, the air roars past you, for you are overtaking the whole world, and shall one day force all nations, all empires to stand aside, to give you way!” - “Que signifie ce mouvement, sujet d’universelle terreur? (...) La clochette tinte d’un son surnaturel; l’air scindé, brisé, gronde, tournoie, s’échappe en ampes courants; tout ce qui est sur la terreest traversé au vol... et l’on voit se retirer de biais, seranger à l’écart et te livrer passage, peuples, royaumes etempires.” - “¿Qué significa este aterrante vuelo? ¿Cuál es el desconocido poder deestos corceles, sin igual en el mundo? ¿Hay torbellinos en sus crímenes? ¿Hay una oreja sensitiva, alerta como una llama, en cada fibra?... La troika vuelta, inspirada por Dios... ¿A dónde vas tan de prisaentonces, Rusia? ¿Dame una respuesta! Pero Rusia no responde. Con un tilin maravilloso suenan las campanillas; el aire cae hecho jirones, truenan y se convierte en aire; todas las cosas del mundo quedan detrás de nosotros y, mirados de soslayo, todos los demás pueblos y naciones se apartan del camino y le dan el derecho de paso.” - «Что значит это наводящее ужас движение? и что за неведомая сила заключена в сих неведомых светом конях? ... Русь, куда же несешься ты? дай ответ. Не дает ответа. (...) Летит мимо все, что ни есть на земли, и, косья, постороняются и дают ей дорогу другие народы и государства».

Nikolai Gogol, “Dead Souls”
What are the key issues in focus of the agenda of the Collective Security Treaty Organization (CSTO)? How has the structure and the governance model of the CSTO changed over the recent years, and what new priorities have emerged for its members? These questions also touch upon the evolving approach of the Organization towards countering the challenges to regional security, fueled by the international terrorism, extremism and others threats which highlighted by the CSTO Secretary General in his interview.

The expert community is increasingly raising the question of whether Russia should withdraw from the 1987 Intermediate-Range and Shorter-Range Nuclear Forces Treaty (INF) today. Potential Russia’s pullout from the Treaty has been discussed since 2003. The issue remains controversial as the treaty is claimed to be detrimental to Russian national security. At the same time, the idea of initiating the collapse of yet another disarmament treaty raises serious concerns over its probable impact on strategic stability. Besides, a thorough analysis shows that unlike the ABM Treaty, the INF Treaty does not hamper Washington’s defense plans, and this fact leaves certain window of opportunities for the Treaty’s future.

The implementation of the State Armament Program to 2020 in Russia results in a massive renovation of weapons and military equipment in a scale, which is unmatched in the modern Russian history. The ambitious program reflects the undisputable priority of technologically upgraded and strengthened Armed Forces. However, the question remains open on how realistic the SAP-2020 targets and plans are — and it becomes even more topical as the international situation undergoes extensive deterioration. Can the Russian defense industry deliver such a massive increase in defense R&D and manufacturing under the press of sanctions? These questions also become vital for further progress of the SAP-2020 and successful launch of the new armaments program for the 2016–2025 period.

Over the recent years, Myanmar made several steps on a winding path of economic and political transformations. The government made a bid on opening of the national economy in order to attract foreign investors, and this strategy resulted in impressive investment boom. However, the experience of several years of Myanmar mania also reveals pitfalls and peculiarities of massive investments in this new national market. The current experience of major powers’ cooperation with Myanmar offers valuable lessons for Russia. Moscow and Naypyidaw share a significant historical background of economic and trade cooperation, and have perspective tracks and formats of its further development — but only if the mutual risks are well understood and mitigated.

The information technology revolution is going on, transforming the landscape of global development and international security in an unprecedentedly fast way. From 3D printing and augmented reality to cyborgization and predictive analytics, the digital technology generates new opportunities and new challenges for the world community. Where does this megatrend of digital progress lead the humanity? Should we get prepared for adapting familiar social, economic and security processes to the rise of artificial intelligence and the prologue of technological singularity?

Amid the ongoing confrontation with the West, Russia’s foreign-policy course is pivoting towards the East, with the growing market of the South-East Asia promises opportunities for partnership in a number of areas, including peaceful nuclear industry. At the same time, Russia remains a quest in the region and it still must work out a formula of its involvement and participation in Southeast Asia. A successful strategy for cooperation with the regional countries should take into account major risks and challenge in the region such as the Fukushima syndrome, the lack of human resources and increasing competition both with alternative sources of energy and foreign market actors in the nuclear energy segment.