



LIFE AFTER NUNN-LUGAR

The U.S. Cooperative Threat Reduction program, also known as the Nunn-Lugar program, has already reached a ripe old age, by the standards applied to such initiatives. Launched in 1992, it played an important and sometimes indispensable role throughout the 1990s in preventing the proliferation of nuclear weapons and WMD components, as well as sensitive know-how, from Russia and other former Soviet republics. The program was conceived during a transitional period in Russian statehood, and it was especially helpful during the turbulent years when Russia was struggling to finance even the most basic nuclear security measures.

The program was launched on June 17, 1992, when Russia and the United States signed the Agreement Concerning the Safe and Secure Transportation, Storage and Destruction of Weapons and the Prevention of Weapons Proliferation. The agreement entered into force on the same day (no ratification by the Russian Duma was necessary), and remained in force for an initial period of seven years. It was extended for another seven-year term in 1999 and then again in 2006. In October 2012 Russia decided against another extension; the Nunn-Lugar program is now due to expire in May 2013.

It is important to emphasize that as recently as in the early 2000s the program was still yielding tangible results. In 2002 it gave rise to the Global Partnership, a nonproliferation initiative spearheaded by the G8. Some 7,659 strategic nuclear warheads had been dismantled as part of the program as of August 2012, in addition to 902 intercontinental ballistic missiles, 191 mobile ICBM launchers, 498 ICBM missile silos, 155 bombers, 906 nuclear air-to-surface missiles, 684 submarine-launched ballistic missiles, 33 nuclear submarines, 194 nuclear test tunnels, and more than 2,937 tonnes of chemical weapons eliminated in the Cooperative Threat Reduction framework. The program has also provided assistance for 578 operations to transport nuclear weapons by railway; stronger security measures at 24 nuclear weapons storage facilities; and 39 newly built and fully equipped bio-threat monitoring stations.¹

Nevertheless, Russia has been not just a recipient of assistance, but also a donor since the early 2000s. It has been a decade since American experts and their Russian counterparts representing the PIR Center gave the following unambiguous recommendation: “Cooperative Threat Reduction must be transformed from a program of assistance to Russia to a program of partnership with Russia; it cannot survive otherwise.” Unfortunately, that recommendation has never been fully implemented.

The importance of the Nunn-Lugar program has been steadily declining in line with the increase in Russia’s own financing of nuclear security. Only recently Cooperative Threat Reduction was useful as a means of plugging the holes in the budgets of the Russian MoD and the state nuclear company, Rosatom. Now, however, the MoD, Rosatom, and the Russian government as a whole have all but lost interest in the program. Its only remaining advocates in Russia are the top managers of some individual companies and research institutes which have become addicted to aid. In its current form, however, that aid does more to corrupt than to help.

Let us not pretend, therefore, that the program has fallen foul of the Russian MoD’s and Foreign Ministry’s intransigence. The truth is, Cooperative Threat Reduction has been very useful—but it has already served its purpose, and now the time has come to lay it to rest. But we absolutely must not lose sight of that program’s truly invaluable experience, both positive and negative. That experience can soon be put to excellent use in the former Soviet republics and—who



knows?—perhaps on the Korean peninsula and in other parts of the world as well, when the time is right for it.

It would be extremely short-sighted of Russia simply to let the program expire this year, and leave it at that. Such an approach would be a repeat of the mistake Russia has already made with the International Science and Technology Center. As soon as the Nunn-Lugar program ends, it should be replaced by a new 10-year program of U.S.–Russian nuclear cooperation, albeit on a significantly smaller scale in terms of spending and the number of individual projects involved. The new program should pursue the following goals:

- ❑ preserve the expertise gained over the previous years and put it to productive use;
- ❑ facilitate cooperative investment in human resources so as to enable current and future generations to make the best possible use of hardware and knowledge provided as part of the Nunn-Lugar program and Global Partnership;
- ❑ spearhead cooperative efforts to use all the accumulated experience in other parts of the world.


The new agreement should prioritize the use of the expertise gained as part of the Nunn-Lugar program for new projects in third countries. The potential candidates include the CIS states (Central Asian republics and Ukraine), which would benefit from measures to improve nuclear security at their nuclear industry facilities. In the Middle East, Russia and the United States could pursue joint projects to give the former nuclear, chemical, and biological weapons scientists new training, which would enable them to find employment in the civilian industry. In Sub-Saharan Africa the two countries could launch joint efforts to prevent bio-security threats (including natural and made-made epidemics). Finally, Russia and the United States could spearhead a project to prevent WMD proliferation in Pakistan, Afghanistan, and Southeast Asia.

By retiring the U.S. programs of assistance to Russia we are not only putting an end to what has become an anachronism, but also eliminating the contentious problem of liability for damage. Let us recall that, as part of the program, the 1992 agreement absolves U.S. contractors working in Russia of all legal or financial liability for damage that may result from their actions or from any malfunctions of the equipment they have installed. In other words, these contractors are not liable for any incidents or emergencies caused by their actions. Moscow has repeatedly demanded a revision of that clause—but Washington has always resisted such demands. Another thing which has long irked the Kremlin is that about 40 percent of the money allocated by the United States for the Nunn-Lugar program has gone to American contractors and consultants instead of being spent on things Russia really needs. Now, however, Russia and the United States will have an equal say in setting the rules of the game for third-country projects.

Moscow and Washington have both declared that, in principle, they are ready to replace the Nunn-Lugar program with a more up-to-date format of cooperation. Nevertheless, the two sides are unlikely to reach a new agreement before the expiration of that program in May 2013. That will inevitably cause a legal vacuum which could affect other important U.S.–Russian agreements, such as the 2010 plutonium disposal agreement or the 1997 program for improving the effectiveness of nuclear material protection, control, and accounting.² Both of these instruments rely on the legal framework set up by the Nunn-Lugar program, although the Russian Foreign Ministry gives an assurance that the expiration of the program will not entail a Russian withdrawal from all the related agreements.

I believe that it should be possible to draft a new U.S.–Russian agreement over the next six months, in time for the meeting between the Russian and U.S. presidents on the sidelines of the September 2013 G20 summit in St Petersburg.

For more analytics on disarmament, please, visit the section “Ways towards Nuclear Disarmament” of the PIR Center website: disarmament.eng.pircenter.org

Retiring the Nunn-Lugar program without a joint U.S.–Russian effort to lay the foundations for a successor program would be an isolationist move on the part of Moscow—and isolationism is the last thing Russia needs at this moment. 

Vladimir Orlov

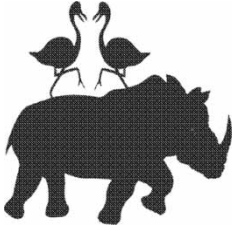
NOTES

¹ Kozichev Evgeny, "How the Nunn-Lugar Program Worked," *Kommersant* No. 190 (4975), October 10, 2012, <<http://www.kommersant.ru/doc/2040919>>, last accessed February 20, 2013.

² Elena Chernenko, Ivan Safronov, and Kirill Belyaninov, "The Nunn-Lugar Account to be Sent to the Russian Finance Ministry," *Kommersant* No. 195 (4980), October 17, 2012, <<http://www.kommersant.ru/doc/2046228>>, last accessed February 20, 2013.



F R O M T H E E D I T O R



Nikolay Spassky

NUCLEAR ENERGY AS A TOOL TO PROMOTE PEACE AND SECURITY IN THE MIDDLE EAST

The 2010 NPT Review Conference reaffirmed the importance of the Resolution on the Middle East adopted by the 1995 Review and Extension Conference, which called upon all countries in the region to take practical steps aimed at making progress towards the establishment of a Middle East zone free of weapons of mass destruction (WMD), and their delivery systems. Steps towards establishing a WMD-free zone in the Middle East region include strengthening institutional nuclear cooperation in the region through the creation of a universal structure that would include every country in the region.

What is nuclear power in the Middle East and how is that related to the problems of the WMD-free zone? How can nuclear energy cooperation help the establishment of a nuclear-free zone in the Middle East? And what is Russia doing in this respect?

We have put these questions to the Deputy Director General of Russia's Nuclear Energy State Corporation Rosatom, Amb. Nikolay Spassky.¹

SECURITY INDEX: What's Russia's approach to nuclear energy development in the Middle East countries?

SPASSKY: Nuclear power itself is neither good nor bad. It may become one or the other depending on what you do with it. The official stance of Russia, and that's my personal conviction, is that we categorically disagree with the concept whereby nuclear power development in the Middle East as a process is viewed as an absolute evil. This is not true. With all the instability in the Middle East, development of nuclear power generation has proceeded quite intensively in the past few years. At least some efforts were made to look into this problem. We believe it to be a quite normal process.

To take a different position and to oppose development of nuclear power generation in the Middle East would be wrong from a formal, from a legal point of view, because that would be outright discrimination and we have commitments that are sealed in a number of fundamental international instruments. In the Non-Proliferation Treaty, we have Article 4 and there is an approach in principle that proceeds from the premise that the international Non-Proliferation Treaty is based on three pillars. One of them is nuclear nonproliferation proper, with all the mechanisms and arrangements that go with it. Second, commitments to move to nuclear disarmament. Third, development of peaceful nuclear energy and international cooperation in this area. In addition to this fundamental legal factor, as we see it, from the practical point of view it would not make any sense to try to stop the development of nuclear energy in an individual, isolated region of the world even if it is as unstable and unpredictable as the Middle East.

We could argue in abstract terms regarding some rich countries of Western Europe whether it would be legitimate on their part to abandon plans to develop atomic energy. But, speaking about countries that address challenging tasks of modernization, and sustainable development, the prospect of abandoning nuclear energy would be burdensome and counterproductive. Even if we assume theoretically that we could and might try to deny the countries of the region the right to



I N T E R V I E W

develop nuclear energy, that would lead nowhere in terms of achieving specific results because thereby we would have pushed those countries into the grey area outside international verification mechanisms and that would be to the detriment of stability, nuclear security, and peace in the region.

Therefore, the position of Russia is quite obvious. We advocated broad-based international cooperation in this area and on the practical plane we have cooperated with a whole range of countries in the region. However, having said that, I must make a provision. We are doing that strictly observing the international law, basis, and framework in two respects: nuclear nonproliferation and nuclear security. These are things that are rather close, one to the other. However, genetically and in substance, these are two different systems.

SECURITY INDEX: focus briefly on nuclear security and nuclear nonproliferation. How did the Fukushima crisis impact Russia's perception of nuclear security?

SPASSKY: Understandably, compliance with the entirety of nuclear safety requirements and rules that have evolved particularly after the Fukushima events is a top priority and an important condition for complying with these requirements. So we are talking about the establishment of a normal infrastructure. And by infrastructure we mean the legal infrastructure as well from the point of view of the actions taken by the national regulators in the nuclear energy field and the infrastructure in terms of the elementary hardware. This involves grades and networks and a number of other things: training of experts, and the safety of nuclear research reactors and nuclear research facilities. These requirements have evolved and have been changing in recent years with the active participation of Russia. There has been a broad discussion following Fukushima and this discussion has been taken to a completely different level. True, Fukushima was a very major tragedy but this tragedy awakened many of us, making us aware that a rosy attitude toward nuclear energy is inadmissible.

The very term “nuclear renaissance”—often abused by many of us—is not the best way to describe this phenomenon because nuclear energy is a very serious thing and can only be pursued and used provided that a whole number of important conditions are observed. One of these conditions is nuclear security, which is fair for any country, and is particularly relevant for the countries of such unstable regions as the Middle East.

When we speak about nuclear security, incidentally, we have some problems in the Russian language because there is “nuclear safety” and “nuclear security” in English. By nuclear safety we mean the safety of the nuclear facility itself. So, now we are building very strict and rigorous regimes that the international community has been moving towards since the time of Chernobyl. Chernobyl became sort of the breaking point in designing that regime and these very serious arrangements. In parallel, there are other regimes that are closely related to this one but are still rather independent. This is what we call nuclear security.

SECURITY INDEX: How does the nonproliferation regime provide the framework for international energy cooperation?

SPASSKY: Nuclear nonproliferation over the past few years has evolved a whole system of requirements that make it possible for international cooperation in the nuclear field to develop. An absolute must without which nothing can happen is of course membership in the Nuclear Non-Proliferation Treaty of a particular country that is interested in developing its own nuclear energy program. This is something fundamental; this is a basic requirement on which everything else is built. Then come the IAEA safeguards on materials and so on. This is something related to our cooperation and we are talking about supplying fuel for the entire lifecycle, and the repatriation of fuel. We are doing this in accordance with international requirements and such guidelines of the nuclear power countries. This has been written down; and these are very tough requirements on non-transferrable technologies and sensitive materials. Well, we believe in this—I know that other countries apply other approaches—and our position is that in its entirety this system of requirements will provide certain guarantees and safeguards that will let us use nuclear energy peacefully.

By the way, my colleagues who out of curiosity or professional interests were looking into the framework agreements on the peaceful use of nuclear energy that we have with other countries, with some of the countries of the Middle East among others, have noticed that the requirements on nonproliferation are something like an icon-stand and, well, it's an entire system. The Ministry for Foreign Affairs of Russia, the Rosatom colleagues responsible for nuclear control, have been doing this and I am boasting about this but there is nothing bad about it and I believe that the Russian system of controls in the domain of nuclear cooperation and nuclear security is not only one of the toughest but one of the best-built in the world. I believe that it is very disciplined and organized. The more simply these things are written down and explained, the easier cooperation will go.

SECURITY INDEX: What's the Russian position on the establishment of a WMD-free zone in the Middle East? How do you see the development of nuclear energy in the Middle East within the context of a WMD-free zone?

SPASSKY: The establishing of a nuclear-free zone in the Middle East is a very important task but not a target in itself. This is a task that is part of the system of efforts that many countries are making internationally. We apply this to the Middle East as a region. The very idea of establishing such a zone is a very important element of promoting a system of peace and security within this region as a whole.

I believe that broad, international cooperation to use nuclear energy peacefully, living up to only the necessary requirements, cannot harm us. And, moreover, in the long term, it will be improving peace and security in the Middle East. I understand that this is a controversial issue. Many people would argue against this but I will tell you why we in Russia think this way.

First of all, the development of international cooperation that will be well disciplined in the use of nuclear energy will make it possible for us to understand the very nature of nuclear energy. Nuclear energy is something very specific. Only robust cooperation, exchange between scientists, circulation of staff, a transfer of staff, a legal basis and so on, all this together makes it possible for us to do away with the illusions that are related to nuclear energy and the nuclear sector as such. Any mistake in this domain maybe based on some simplified understanding or a misunderstanding.

Second, international cooperation in the nuclear sector makes it possible for countries that are developing their nuclear programs to become part of the transparent international mechanisms working in the nuclear sphere. I'm talking about the safeguards that are built within the system and it's not only about agreements. I'm talking about aerial filming, about Code 31, about conventions, about the Convention on Nuclear Security, the Convention on Early Notification of a Nuclear Accident, and the Nuclear Safety Convention. I believe it is as revolutionary as the initial protocol on applying these safeguards as well.

I don't want to pinpoint any countries on the map of the world that are participating or not participating in these conventions, and this is not important. The most important thing is that we are monitoring this system and the task related to the participation in these mechanisms should be universal.

Nuclear power plants and nuclear power reactors have a long lifecycle, up to 100 years I would say. First we have to build a nuclear power plant—it takes about 10 years—some 60 years is the normal lifecycle of modern nuclear reactors of the 3.5 generation. Then decommissioning and waste disposal and so on, taken together, is about 100 years. The cooperation that we are building for another 100 years is bringing a new format to our thinking. It brings in new algorithms.

Nuclear energy needs a peaceful external environment to develop in a normal way. Nuclear energy and military conflicts are incompatible because of the nature of the nuclear power plant. This understanding does not come automatically. It's not like clicking a button and everyone understands this. But when we start cooperation and start talking about this past experience and getting new information, countries and experts change their thinking drastically.

SECURITY INDEX: How do you see the nuclear energy as a resource of modernization, especially in the Middle East region?



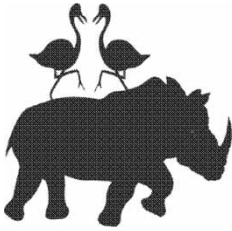
SPASSKY: If applied to countries that need strong incentives to develop their economies, such as the Middle East countries, nuclear energy is a very serious resource for modernization. I'm not idealizing this situation, and everyone has his or her own ethical stand and his or her own understanding, but I am not talking about specific situations, I'm talking about power plants, and the power energy sector, the health sector, isotopes, innovations, agriculture, and just employing people. We're talking about many thousands of people who are trained, who get new experience, and then they become part of the core innovational drive in their countries. We in Russia believe that well-thought-out cooperation in the nuclear sector promotes stability and peace in the world and makes it possible to promote peace and security in this conflict-ridden region.

We have been working with the Middle East a lot. We will be working with Middle Eastern countries. We will cooperate in the name of using nuclear energy peacefully but this will be done under the very tough control of compliance with the regulations on nonproliferation and nuclear security. And if these requirements are complied with cooperation will continue. If not, we will stop any cooperation. This kind of work, separate from other kinds, will become part of our effort to establish a nuclear-free zone in the Middle East.



NOTE

¹ The interview is based on Amb. Spassky's speech at the international seminar, "2012 Conference on the Middle East Zone Free of Weapons of Mass Destruction—Searching for Solutions," held by PIR Center on October 4, 2012 in Moscow.



Jamie Saunders

HOW TO AVOID CONFLICT ESCALATION IN CYBERSPACE

Is it possible to establish a legally binding international regime in the field of cyber security? Could the Budapest Convention on Cybercrime be regarded as a potential basis for establishment of a global mechanism aimed at countering cybercrime?

We have put these questions to the Foreign and Commonwealth Office Director for International Cyber Policy (UK) Jamie Saunders.

SECURITY INDEX: What's your assessment of the Russian concept of a global UN Convention on cyber security, presented at the London Conference on Cyberspace in November 2011? What changes should be introduced to the Russian draft document in order to make it a sound basis for further debates and negotiations on a future regime for the international security of cyberspace?

SAUNDERS: The first thing I should say is that we welcome the very fact that Russia became interested in a dialogue on these subjects. Russia has been actively participating in the work of the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. And as you say, the Russian proposal was presented a year ago at the London Conference on Cyberspace, so Russia and the UK will come on to bilateral conversations on these issues later this year. I think where we begin to have concerns is the question whether it is premature now to be actually proposing an international legally binding document at this stage—that's our first concern. And the second concern is when we start looking at how we address these issues and how to avoid escalation [of conflicts] in cyberspace. We do need to find a way to engage beyond governments, to engage the IT industry and civil society because each of these actors has an important stake in it. And the contribution they could make in terms of confidence building, sharing information, crisis communication, etc.

SECURITY INDEX: Just to clarify some of the points you just mentioned—hasn't the time already come to forge some legally binding regime of information security after a number of destructive malwares like Stuxnet, Flame and Duqu were released and caused physical damage to critical infrastructure in some states like Iran?

SAUNDERS: We certainly agree that international law should have something to say something about issues like that. I think the question of further debates is whether we need something or whether it's a matter of how successfully we apply already existing international law—laws of armed conflicts and so on—to the agenda of cyberattacks. I certainly think that existing international law is relevant and important in the sort of scenario you just described. The question is, should we at this stage be seeking to negotiate a new instrument or should we keep focusing on the capability of existing instruments—and we believe we should be doing the latter.

SECURITY INDEX: Could the Budapest Convention on Cybercrime be regarded as a potential basis for a global and comprehensive regime of international cooperation against cybercrime? What terminological and conceptual updates should be introduced to the text of the Convention in order to adapt it to the present-day landscape of transnational threats of cybercrime that has changed greatly since 2001?



SAUNDERS: The first thing I would say is that we see it as a very important that countries throughout the world—first—have up-to-date and modern cybercrime legislation, and second that there are mechanisms in place in order to enable international cooperation on tackling cybercrime, and I think most countries would agree with that. As far as we can see it, the Budapest Convention does provide a good articulation of what the countries need to do. And we also continue to support this document as a sort of a blueprint in terms of what good national anti-cybercrime legislation looks like. I recognize that the Convention is more than ten years old now and it needs to be updated. In fact there is a mechanism that enables it to be updated—Article 44 of the Convention itself. We haven't seen any updates yet, and no changes were introduced to it yet. I think the key thing is that we do think we need to make changes and we need to make them as technologically neutral as we can. I mean we have this with our domestic anti-cybercrime legislation as well, but the more general the legislation is the more long-lasting it is. So I think it is of great importance that we have a mechanism for updating the Budapest Convention. I think such a mechanism already exists in Article 44, and it's interesting why the UK hasn't seen the need to use that article yet.

SECURITY INDEX: Are there any other potential documents and initiatives that could possibly substitute the Budapest Convention as a potential blueprint for a global anti-cybercrime regime, probably UN-based?

SAUNDERS: I think that what really matters is the actual content of the Budapest Convention—in other words, its provisions which we see in a sense of providing a baseline. And any additional proposal forthcoming we would need to judge against that. So if any new initiative doesn't suggest certain things instead of those lacking in the Budapest Convention which were not appearing but we thought were very important, it would be very hard for us to support that. In other words we think that the Budapest Convention provides a benchmark for cooperation against cybercrime. Obviously, if there is a universal agreement or other instrument that provides a better cooperation mechanism than the Budapest Convention then we would be supporting it. And that's the key question—if what's being provided brings improvement to the Budapest Convention then obviously we are going to look at it. If we fear it just falls short of the provisions of the Convention then we are likely to have serious concerns about it. Once again, we are not saying the Budapest is perfect by any means—and at least there can be improvement—and that's how we see any initiative coming out. One more thing I would like to add is that there are not so many differences between Russia and the West in terms of how to get to the end result in the field of information security and tackling cybercrime internationally. But I think that an agreement with Russia only needs to improve international cooperation on cybercrime and to ensure that we have the right environment with our colleagues to maintain, in order to strengthen the stability of the cyberspace itself. I don't think we have any fundamental disagreements about the outcomes of our cooperation.

SECURITY INDEX: The key stumbling block between Russia and its Western partners when it comes to cyberspace is a major terminological and ideological gap between Russian and Western concepts. Russian experts prefer to speak about information security instead of cybersecurity—which is much broader field for analysis and regulation. Which of these two approaches seems to be more relevant for the purposes of global regulation of cyberspace? Are there any chances that the Russian concept of information security is understood and accepted in the West—and namely in the UK?

SAUNDERS: I would distinguish two aspects of the issue. The first is the issue of language itself and I agree it has caused some difficulties that can slow things down in the international dialogue. I think the A-way to make some progress for us is to be clear with each other—I mean namely the UK and Russia and other players—about precisely what they mean by the language they use. And obviously we have translation challenges as well but it's going to be worth us actually sharing all definitions, because we are making assumptions about what each other mean. I guess the more we can spell out what we mean the more we can get over in the sense of the words themselves and get towards their true meaning—and that's just something we are proposing. I don't think we will reach common definitions in terminology in a short-term prospect, but we can still share what we mean by our terminology. And if that happens we'll be able to identify genuine differences and where we are actually misinterpreting what each other is saying.

The second point I would like to make is that there are genuine differences behind the language. In terms of what we think should be subject to the international discussions on cybersecurity that are taking place now. And it seems that here the British politicians and experts misunderstood

what the Russian language meant. We should say that the definition “information security” widely used by the Russian side relates directly to the content of communications and that actually what the dialogue here is mostly about is restricting the freedom of expression in cyberspace in a way that we think would run counter to the obligations we both made on the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights, which the UK and Russia are both parties to. So if we could become clearer in terms of what exactly we mean by the different language we use and if we can identify whether we are talking about different things or whether we just misunderstood each other. But I wouldn’t like to underplay all or some existing differences of views—specifically around the issue of content.

SECURITY INDEX: The recent cases of the Stuxnet and Flame sophisticated viruses invading well-protected objects in the Middle East and world over prove that new extremely massive and sophisticated types of malware are likely to be widely used in coming years by unknown actors. Does the British government consider such malwares as a major threat to national security? What steps have been made by the FCO to prompt discussion of this problem in the international arena?

SAUNDERS: First of all, you highlight Stuxnet and Flame specifically in your question and I wouldn’t say that we consider those specific cybertools as a threat to our national security. But we do see that there are threats or potential threats of malware and in that sense it can be regarded as a national security issue. And the potential of modern malwares to cause significant damage to the critical national system is very real. The UK security services have not yet faced such malwares as Stuxnet and Flame being targeted against Great Britain but it doesn’t remove the point that malicious malware could cause serious damage to our critical national infrastructure, and it’s something we do recognize and accept. In terms of proper reactions to such a threat we are, as might have been expected, very active at the UN GGE on ICT security discussions on this issue. We also have seen some of the activities and been supporting some of the activity in the OSCE and in the Asian Regional Forum and taking a look at their approach to these issues. And in terms of confidence-building measures—we think there is an important and legitimate subject for governments to be talking to each other about and to see how we can prevent what I think we all want to avoid, which is an escalation of this malware’s capabilities and real damage to our critical national infrastructure systems. And finally of course we hosted the London Conference on Cyberspace a year ago in 2011, and the issue of destructive malwares posing a threat to critical systems was one of the subjects which were addressed within its framework. And this issue will be addressed once again in the Budapest conference on Cyberspace in October 2012 and at all major cybersecurity events next year. I don’t want to say it’s the only issue worth being discussed but it’s important we discuss it at the level of governments so that these issues will be exposed to our leaders.

SECURITY INDEX: As you pointed out, malicious programs are considered to be a major threat to national critical systems. And what segments of it are regarded as the most vulnerable ones: the power grid, banking information systems, etc.?

SAUNDERS: That’s a difficult question to answer. I mean, in what you ask you combine the degree of vulnerability of the system and the impact of the system to a society as a whole. So in fact there is hardly any sort of simple ranking of national critical infrastructure segments in such a way. But there is no doubt that such things as the electricity and power supply, food distribution, and similar systems are the sectors where we require the highest level of assurance that the system is secure and properly protected. And we do define our national critical infrastructure in different sectors—and it highlights where we think the biggest problems and most serious challenges might take place. I also think it’s important not to look at cyberthreats in isolation either, because actually we need to protect such systems as our electricity grid from a wide range of threats, both non-human and man-made, both cyber and physical. So we try to take a complete, comprehensive view of that and to apply risk management principles on that basis.

SECURITY INDEX: When it comes to massive and well-orchestrated cyber attacks the key problem is the anonymity of their authors—despite the fact there a few states to be under suspicion in most cases, including China, Russia, the USA, Iran etc. Did British governmental networks ever face such attacks and if yes, was the issue of attribution solved successfully? Did the FCO (or the British government) ever happen to claim any nation-state to be directly responsible for cyber attacks and if yes, what was the reaction?



SAUNDERS: First of all, like many other countries we are subject to regular cyber intrusions into our networks. I think we've quoted figures in terms of the government networks sector—for example, there are hundreds of thousands of attacks targeted against only some of our government networks. So as you can see, there's a lot of activity out there, and attribution is difficult—but it's not impossible, a long way off impossible. So far we haven't chosen to—it's not easy to choose a proper term—blame any nation state to be directly responsible for cyberattacks. We have not engaged in any official public naming or shaming a country we think is behind those attacks. The key point here is that when we believe a country is all involved in that sort of activity we do have the right to take action in response, consistent with our rights and obligations stated in international law. If we think we are being attacked we are certain to do something about it. This reaction will take place on all sorts of different levels, and it would certainly include some measures to be undertaken in the diplomatic arena.

SECURITY INDEX: What are the key points in the FCO's agenda when it comes to promotion of international cooperation in the cybersecurity area? Are there any global initiatives or perspective strategies for international cybersecurity cooperation to be elaborated and presented by the FCO in the nearest future? What are the FCO top cybersecurity priorities to be promoted next year?

SAUNDERS: I would like to mention two things specifically here. The first is that from my point of view there is still more work to do in the field of raising awareness on these issues—on the top level within governments and businesses and in the civil society, and the natural target audience is for example business leaders across the world. We really understand this is a serious threat that we are facing and I mentioned our conference in London last year where this approach was exercised. We are regularly talking to partners about this problem—raising awareness, offering assistance and so on and so on. There's a lot to be said for a country like the UK, actually, helping or prompting partners across the world to understand that this is a serious issue that they need to tackle.

The second thing that we are looking at is to see how our own specific experience and skills can be used to help other countries develop their own capabilities and capacity. For the moment we are already funding a number of initiatives within the framework of which we are providing not only money but our expertise. But we think we are to do more. I think it's important to make sure we're getting the impact on the global capacity-building agenda that we need.

SECURITY INDEX: Do you have any specific regional priorities of international cooperation in the cybersecurity area? Are there any regions being considered as a basic and crucial direction in terms of such cooperation?

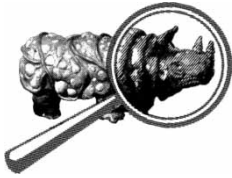
SAUNDERS: It's quite hard to prioritize as different scenarios require different things and obviously our very top priority is securing our own critical information systems. And only then are we looking to see what the other countries are that need our help most of all. Some of them—and it's an example of where we are funding some work in this direction—are some states in South East Europe we are cooperating with. We are also funding work that the Council of Europe has been doing on helping countries of Eastern Europe willing to join the Budapest Convention on Cybercrime to develop their legislation in the cybercrime area. We are supporting work within the framework of the Commonwealth aimed at capacity-building and expanding law-enforcement capabilities in the cybersecurity field. But that's the start and I think we do see the need to do more and we need to make our further efforts to a very great extent driven by an assessment of where it has to make greatest impact. One of our concerns here is that there is a lot of different programs are out there that do not really give the impacts which we expect the impacts have to be.

And I also would like to return to your earlier question in terms of international debates. There are international debates on laws and global agreements in cybersecurity but there is also another area which is important in terms of promoting international cooperation in this field.

For more analytics on information security, please, visit the section "International Information Security and Global Internet Governance" of the PIR Center website: net.eng.pircenter.org

Building confidence, building transparency, building trust and other suchlike things provide the environment in which international cooperation on tackling common cyberthreats can be held.





Anatoly Antonov

FURTHER NUCLEAR ARMS LIMITATION: FACTORS AND PROSPECTS

The New START treaty between Russia and the United States has entered into force. Under the terms of the treaty, by 2018 the Russian and U.S. strategic offensive arsenals will be brought below the new ceiling of 700 deployed delivery systems and 1,550 warheads deployed on these systems.

The treaty stipulates a large number of measures which must be accomplished within a clearly defined time frame. The implementation of some of those measures began even before the ratification; others have yet to be rolled out. Several of the measures agreed in the treaty have already been implemented. First and foremost, Russia and the United States have exchanged initial data on the composition and the location of their strategic offensive weapons arsenals at their military bases. They have also put together teams of inspectors and conducted several demonstrations stipulated by the treaty. They have begun inspection visits under the new procedures. Finally, they have launched a consultation mechanism in the framework of the Bilateral Consultative Commission (BCC). Experts and officials attending the commission's sittings discuss practical issues pertaining to the implementation of the treaty. During the winter 2012 session of the BCC (held on January 24–February 7) they “signed agreements about exchanging telemetry information for ICBM and SLBM launches, to be submitted by each Party, and about the procedures for conducting demonstrations of information storage mediums and/or equipment for the reproduction of telemetry data.” They have also reached an agreement “about the number of ICBM and SLBM launches for which telemetry information will be exchanged in 2012.”¹

The question is, what next? Are deeper strategic offensive arms reductions after the expiration of the latest START treaty possible, or indeed necessary?

DETERMINING FACTORS

Obviously, strategic offensive arms reductions are not an end in themselves. The notion of such reductions was born at the beginning of the era of nuclear arms disarmament talks, and it had a very clear purpose. It aimed to maintain the security of both parties at lower levels of nuclear arsenals.

It is quite clear that at this moment Russia's security does not depend solely on the balance of strategic nuclear arsenals with the United States. It also depends on numerous other factors, including: U.S. plans for a global missile defense system; the situation with sea-based, long-range cruise missiles and other long-range high-precision weapons; the prospects for the removal of American non-strategic nuclear weapons from Europe; the balance of conventional forces; the numerous military bases with growing military infrastructure in close proximity to Russia's borders; implementation of various ideas for placing weapons in outer space; etc.

Let us focus specifically on the issue of numerical indicators of the Russian and U.S. nuclear arsenals. The indicators for delivery systems are approaching critical levels. I doubt if anyone



A
N
A
T
O
L
Y
S
I
S

would argue that, in the end, the real deterrence capability depends precisely on the numbers of delivery systems, their technical specifications, their resilience and survivability, and many other factors.

The need for the engagement of all countries which possess nuclear weapons in the nuclear arms reduction and limitation process is becoming increasingly pressing. It is important that this realization is becoming part of the broad public and political debate. Public opinion, and the opinion of NGOs and the research community, have become impossible to ignore.

In this context let us recall the ideas voiced by the Global Zero initiative, the Luxembourg and Munich forums, and some other NGOs specializing in global security. The Sustainable Partnership with Russia (SuPR) Group, a PIR Center project, deserves a separate mention. There are many interesting, rational, and constructive ideas in its proposals. Of course, some of the ideas are debatable and contentious. Nevertheless, it is obvious that we must make use of the intellectual potential of such organizations to choose the right strategy for further nuclear arms reduction and limitation.

Another problem lies in the context of the outlook for nuclear arms control. Some weapons systems which affect the strategic balance of power are not categorized as strategic by the existing international legal framework—but their nature is in fact strategic because they are capable of taking out strategic military targets and major command and control centers. As we implement deeper cuts to our strategic offensive arsenals, the impact of such weapons systems on the balance of power will continue to grow.

Take, for instance, high-precision weapons, which are not subject to any limitations in terms of their numbers, performance specifications, or deployment locations, and which are well disguised in terms of their true purpose (portrayed as they are, for example, as an instrument of the war on terror). Such weapons can in fact be used to take out strategically important targets. Thanks to their very short approach time and high precision of targeting, they can be used to deliver a sudden strike, leaving little time for reaction or retaliation.

Can Russia afford simply to ignore all of these factors? Obviously, it cannot talk about a nuclear zero while turning a blind eye to all these problems and their effects. Russia consistently advocates a reduction in the level of nuclear confrontation. Nevertheless, it cannot ignore the fact that, of the many factors which affect military security, the Americans tend to focus only on strategic nuclear weapons, while at the same time undermining all attempts to resolve problems in all the areas in which the United States has the advantage over Russia. With such an approach, achieving further strategic offensive reductions will be very problematic. In these circumstances, rather than strengthening strategic stability, any further Russian–U.S. strategic offensive reductions are more likely to undermine that stability.

The outlook for further strategic offensive arms reductions therefore depends on finding mutually acceptable solutions to other important security problems. The United States must unambiguously indicate its readiness to search for solutions to the problems outlined above. Further agreements on strategic offensive arms reductions will not be in Russia's national security interests unless these solutions are found. It has become quite obvious that in the current situation nuclear weapons are Russia's main instrument for ensuring its national security.

INTERMEDIATE-RANGE AND SHORTER-RANGE MISSILES

In recent years politicians and experts in Russia have been debating the possibility of pulling out of the 1987 INF treaty.

The terms of that treaty and its significance for strategic stability have been discussed in earlier sections of this monograph. Let us recall, however, that the successor states of the Soviet Union as far as the treaty is concerned were Russia, Belarus, Ukraine, and Kazakhstan. These four countries and the United States remain the parties of the INF treaty.

The following arguments have been proposed in favor of withdrawing from the INF. The geopolitical situation has changed radically since the treaty was signed. One of the two original parties to the treaty, the Soviet Union, has ceased to exist. Some of the former Soviet republics and Warsaw Pact countries that used to host Soviet intermediate and shorter-range missiles—which were an instrument of deterrence against NATO—have since become NATO

members or want to join the alliance. The threat of global nuclear war or a large conventional war involving Russia and other leading world powers has diminished. The purpose of the INF treaty was to defuse nuclear confrontation in Europe between NATO and the Warsaw Pact. That purpose has been served, and the original military-political reason for signing the treaty has ceased to exist.

On the other hand, although the likelihood of a global war has diminished, the world has become much more prone to regional conflicts. There is a growing threat of proliferation of nuclear weapons and missile delivery systems, and the new challenge of international terrorism.

For some of the state parties to the INF treaty these new challenges can pose a very real national security threat. Some of the INF parties could counter those threats and minimize their costs by deploying weapons systems which are currently banned under the treaty; this applies especially to intermediate and shorter-range missiles with conventional warheads. Many of these countries have retained the expertise and industrial capability required to build intermediate and shorter-range ground-based ballistic and cruise missiles.

In addition, the situation whereby the five INF parties (Belarus, Kazakhstan, Russia, Ukraine, and the United States) are bound by the treaty while the rest of the world is free to develop intermediate and short-range missiles in order to meet its defense requirements is discriminatory.

That is why Russia has called for a discussion of the possibility of making the INF treaty universal by means of persuading other countries to join it, relinquish their intermediate and shorter-range ground-based ballistic and cruise missiles, and shut down all relevant programs. A joint Russian–U.S. statement to that effect was made at the 62nd Session of the UN General Assembly in 2007.²

Some decision-makers and experts believe that unless other countries heed the call for making the INF treaty universal, Russia should seriously consider exercising its right to withdraw from that treaty. Such a decision could be justified by Russia's need to take additional steps to strengthen its security in a situation which has changed significantly since the signing of the INF treaty.

The balance of power in the area of conventional forces in Europe has changed. This is a topic of energetic discussions in Vienna in the framework of the Special Consultative Group. Experts at the NATO-Russia Council in Brussels are also involved in these debates. The armies of the NATO members and several other Russian neighbors are becoming increasingly capable. New potential security threats have emerged in the vicinity of Russia's borders on the Eurasian continent. These include NATO's eastward enlargement; the development of WMD and missile delivery systems in several neighboring countries; growing tensions near the Russian borders; the growing threat of international terrorism; and many other developments.

In such circumstances Russia could use an arsenal of intermediate range and (to a lesser degree) shorter-range missiles as an additional instrument of regional deterrence and as a way of neutralizing the superiority of NATO and other countries in conventional weapons.

Experts are also discussing another reason for deploying intermediate-range missiles: it is argued that Russia needs to respond to U.S. plans to deploy a missile defense system in Europe. Missile defense facilities in Europe could become potential targets for Russian weapons, and intermediate-range missiles are ideally suited for that task.

Nevertheless, Russia needs to conduct a meticulous analysis of all the pros and cons before deciding whether to withdraw from the INF. Such a unilateral step could in fact lead to serious negative consequences for Russia's own security.

A Russian pullout from the INF could be used as a justification for the deployment of American intermediate and shorter-range missiles in Europe. As a result Russia would once again face a problem which it has resolved at great cost to itself by signing the INF treaty in the first place. Essentially it would create a threat to its own security which is much greater than the missile threat posed by third countries. The new NATO members will not require much persuading to host American missiles. They have already demonstrated their attitude when decisions were being made on the deployment of the American missile defense system in Europe. The deployment of intermediate-range missiles in the early 1980s was seen as a serious threat by the Soviet Union. For Russia, it would be an even greater threat in the current situation. The American Pershing-2 missiles had only about half of the Soviet Union's European territory within their range. If similar



missiles were to be deployed on the territory of the new NATO members, the entire European part of Russia would be within their striking distance.

Many European countries are likely to respond to Russia's withdrawal from the INF treaty by inviting the United States to deploy its missile defense facilities on their territory. The intermediate-range missiles Russia could deploy to take out missile defense sites in Europe would themselves become targets for American missile interceptors. Everything would then depend on the balance of numbers and technical characteristics of the weapons in question.

A Russian decision to deploy intermediate-range missiles would further consolidate NATO countries around their shared anti-Russian sentiment, thereby strengthening the United States' position on the European continent. Russia would once again be portrayed as an enemy.

A unilateral Russian withdrawal from the INF treaty would also be destructive for the entire arms control system. It would have negative consequences for the NPT and the nuclear nonproliferation process as a whole.

Let us now move on to the Russian and U.S. initiative on turning the INF into a global treaty. Establishing and implementing such a regime would yield many benefits.

The world would be free of missiles with a range of 500km to 5,500km. This would result in a radical improvement in the security situation for the entire planet.

Such an outcome would also make an important contribution to strengthening the WMD nonproliferation regime. It is well known that missiles are the best delivery systems for nuclear ammunition. The absence of such missiles would significantly reduce the incentive to develop nuclear weapons. That would be an extremely valuable contribution by third countries to the nuclear disarmament process.

An agreement on a global elimination of intermediate and shorter-range missiles would essentially remove the need for missile defenses against such missiles because that is exactly the class of missiles being deployed by the "countries of concern." Suggestions that such countries could deploy ICBMs remain purely hypothetical.

Combined with a new climate of relations between Russia and the United States, a global INF treaty would be a powerful stimulus for further strategic offensive reductions.

Finally, a global INF treaty would not only strengthen international and national security, but would also relieve the participating states of the economic costs of developing, manufacturing, and deploying intermediate and shorter-range missiles.

Nevertheless, it should be recognized that a global INF regime is not a realistic possibility in the foreseeable future.

On the one hand, many countries see such missiles as an important (and sometimes their main and only) instrument for ensuring their own security or preventing regional conflicts. A case in point is Indian–Pakistani relations. In addition, many countries view possession of such missiles as a way of bolstering their political clout in the regional and global arena.

On the other hand, the initiative to globalize the INF does not include any security guarantees for the countries which agree to relinquish such missiles, or which have never had them in the first place. Neither does it contain any incentives for such countries. Clearly, the countries which have acquired missile weapons have spent huge financial and material resources in the process—and there is not even a suggestion that some kind of compensation might be possible.

Finally, there is another very important question: does the initiative require the participation of every single country—or should only selected countries be invited to join?

Eliminating two classes of missile weapons is, in itself, a good idea. But before we can begin to implement it, we need to discuss the terms, conditions, and principles for negotiating an agreement on the elimination of intermediate and shorter-range missiles. The following considerations must be taken into account, among others:

- We need to recognize the inadmissibility of using force or threat of force to resolve political issues. Policies such as those demonstrated by NATO in Yugoslavia and in the Middle East remain a serious obstacle to the implementation of such an initiative.

- ❑ We need to decide whether the agreement should be universal, or whether individual countries (including some states which possess intermediate or shorter-range weapons) can remain outside the treaty or join it at some later point.
- ❑ The treaty must be signed for an indefinite term.
- ❑ The treaty must necessarily stipulate a step-by-step resolution of the problem over a relatively long time frame (the problem cannot be resolved all in one go).
- ❑ An important staging post on the way to implementing the initiative would be an agreement by all countries to declare their stockpiles of intermediate and shorter-range missiles.
- ❑ The eventual agreement must include national security guarantees for all its participants; a successful outcome is unlikely without such a provision.
- ❑ In addition to security guarantees, it is important to develop and agree measures to reward countries for relinquishing WMD missile delivery systems. These could include, for example, preferential terms for putting their spacecraft into orbit using other countries' space launchers, or assistance in developing their own space launchers.

NON-STRATEGIC NUCLEAR WEAPONS IN RUSSIAN–U.S. RELATIONS

Even before the official talks on the New START treaty had begun, many U.S. politicians were calling for the inclusion of non-strategic (tactical) nuclear weapons on the agenda of the talks.

Their arguments in favor of initiating non-strategic nuclear weapons (NSNW) talks included Russia's alleged numerical superiority in that weapons category; the opacity of Russia's NSNW policy; and concerns over the reliability and security of Russian nuclear munitions.

The scope of the New START treaty does not include NSNW. Even before the New START talks had begun, a joint statement by the Russian and U.S. presidents made in London in 2009 said that "The subject of the new agreement will be the reduction and limitation of strategic offensive arms."³

In fact, NSNW have never been included in the scope of strategic offensive reduction treaties. It is worth noting, however, that when the Russian and U.S. presidents negotiated the outlines of the START III treaty in Helsinki in 1997, they deemed it necessary to instruct their teams of negotiators to discuss possible NSNW measures in the context of the talks.⁴ But, for various reasons, the START III negotiations never took place, so the two presidents' instruction was never implemented.

Nevertheless, politicians in the United States continue to demand a negotiated agreement, which would reduce Russia's alleged superiority in NSNW. They say that without such measures no further progress is possible on strategic offensive reductions.

Such demands are contained in the U.S. Senate resolution on the ratification of the New START treaty. Let us recall that the resolution instructs the U.S. administration to seek, within a year of the 2010 New START treaty entering into force, the launch of Russian–U.S. talks on further nuclear reductions which would also cover tactical and non-deployed warheads. As a first step the resolution proposes mutual transparency and confidence-building measures, including exchange of information regarding the numbers, types, and storage locations of NSNW.

At the same time, the 2010 U.S. Nuclear Posture Review sets out a somewhat different objective—namely retaining the U.S. forward-based NSNW capability, which relies on tactical fighter-bombers and heavy bombers. It also contains plans for extending the service life of the B-61 nuclear ammunitions (about 200 of which are stored in five European NATO countries).⁵ Also, the new NATO Strategic Concept (adopted in November 2010 in Lisbon) says that the alliance's nuclear forces are an especially important element of the deterrence system and a means of demonstrating transatlantic solidarity.⁶

There seem to be good reasons to believe that for now the U.S. administration is not planning any major NSNW reductions. To comply with the Senate resolution, the White House will probably have to do nothing more than to enter, for appearance's sake, into talks with Russia on transparency measures.



Another thing to take into account is that the international community has repeatedly urged Russia and the United States to reduce their NSNW arsenals as part of the NPT review process at the UN. Such calls have been made not only by Western countries but also by some non-aligned nations.

For example, during the 57th session of the UN General Assembly, the assembly's first committee approved a resolution headlined "Reduction of Non-strategic Nuclear Weapons."⁷ The resolution includes the following provisions:

- Reductions and elimination of non-strategic nuclear weapons should be included as an integral part of the nuclear-arms reduction and disarmament.
- Reductions of non-strategic nuclear weapons should be carried out in a transparent, verifiable, and irreversible manner.
- The Russian Federation and the United States are called upon to formalize their presidential initiatives into legal instruments and to initiate negotiations on further reductions.
- Further confidence-building and transparency measures are needed to reduce the threat posed by non-strategic nuclear weapons, as well as concrete agreed measures to reduce further the operational status of non-strategic nuclear weapons systems in order to reduce the danger of those weapons being used.
- The states which possess nuclear weapons must undertake a commitment not to increase the numbers of non-strategic nuclear weapons, not to create or deploy new types of such weapons, and not to develop logical justifications for their use.
- The types of non-strategic weapons which have been removed from the arsenals of the states should be banned, and new transparency measures should be developed to verify the elimination of these weapons.

It is therefore safe to assume that Russia will face growing pressure in the coming years over the issue of non-strategic nuclear weapons. In such circumstances it is very important to formulate a stance on the NSNW issue that would properly reflect the existing situation.

At present the Russian and American non-strategic nuclear arsenals are regulated by the political initiatives announced by the Russian and U.S. presidents in 1991 and 1992.

The October 5, 1991 initiative by Soviet President Mikhail Gorbachev was announced in response to the unilateral American initiative announced by President George H.W. Bush on September 28, 1991. After the break-up of the Soviet Union the Soviet commitments regarding NSNW were reaffirmed by Russia as the successor of the Soviet Union. They were also expanded and fleshed out in a January 29, 1992 statement by Russian President Boris Yeltsin, "On Russian Policy Regarding Arms Limitation and Reduction."⁸

The NSNW commitments included practical measures to cut or eliminate such weapons, and to reduce their operational status. Neither of the two countries specified any deadlines for NSNW reductions. Nevertheless, Russia soon announced the schedule for the elimination of various types of its NSNW, under which all the commitments it had undertaken were to be implemented before the end of 2000.

The key points of the unilateral NSNW initiatives are listed in Table 1.

Implementing these NSNW steps as unilateral initiatives had enabled the two countries to avoid protracted and difficult negotiations, and to achieve progress in eliminating the surplus of non-strategic nuclear ammunition.

According to the Congressional Perry-Schlesinger Commission, Russia and the United States have removed about 14,000 nuclear munitions from their armed forces as part of these NSNW reductions. Neither of the two countries has released any official information about the numbers of non-strategic ammunition that have been eliminated or the numbers still remaining in its arsenals. Russia and the United States do recognize, however, that they have reduced their NSNW stockpiles by 75–80 per cent compared with peak Cold War levels.⁹

Table 1. Russian and U.S. Initiatives on NSNW

Weapons type	U.S. Initiatives	Russian initiatives
Artillery pieces and warheads for ground-based tactical missiles	Removal to U.S. territory and complete elimination	Removal to storage, complete elimination, and end of manufacture
Mines		Removal to storage, complete elimination, and end of manufacture
Weapons for surface ships, multirole submarines, and land-based naval aviation	Removal from delivery systems to storage facilities on U.S. territory, large reductions	Removal to storage, reduction by one-third
SAM warheads		Removal to storage, 50 percent reduction
Air ammunition		50 percent reduction

Neither of the two countries has undertaken any new NSNW commitments since the announcement of the presidential initiatives, and no legally binding international NSNW regime has been put in place.

A number of problems make it difficult to begin NSNW talks. Most importantly, there are political differences with regard to non-strategic nuclear weapons. Because of Russia's geostrategic situation, the NSNW arsenal is a lot more important to Russia than it is to the United States. Moscow views its NSNW as a way of neutralizing NATO's large conventional superiority in Europe.

Another important argument is that Russian non-strategic nuclear weapons are an instrument of deterrence against third countries which have missiles capable of reaching targets in Russia. For the United States, on the other hand, the only threat comes from the strategic arsenals of Russia and China.

A very important thing to take into account is that all Russian NSNW are stockpiled on Russia's own territory; these weapons have been removed from the armed forces and are being kept at special storage bases. The Russian non-strategic nuclear weapons therefore pose no threat to the United States.

In contrast, the United States has NSNW stockpiles in Europe, in close proximity to Russian borders. Essentially, these weapons have strategic capability because they can be used to take out strategically important targets on Russian territory.

At its summit in May 2012, NATO decided to leave American NSNW in Europe, although members of the alliance also said they would work to put in place the necessary conditions for "further reductions." It appears that NATO has not overcome its internal divisions over the pullout of American bombs from Europe—but for now a decision has been made to leave things as they are. NATO's Deterrence and Defense Posture Review (one of the main documents approved at the May 2012 summit) includes a rather vague-sounding passage about studying possible concepts for participation of members of the Nuclear Planning Group in implementing agreements on nuclear sharing.¹⁰ However, NATO members make any changes in that area conditional on new NSNW reduction steps by Russia.

It is not difficult to understand the Russian position voiced during UN GA sessions and NPT review conferences; Moscow says that the United States must remove its NSNW from Europe to its national territory and dismantle the requisite NSNW infrastructure in the non-nuclear European NATO countries.

Russia's demands to remove American NSNW from Europe and dismantle the NSNW infrastructure on the European continent are portrayed in the West as an attempt by Moscow to weaken NATO, and a demonstration of Russia's unwillingness to discuss NSNW reductions in earnest. Some Russian experts also believe that such an approach by Moscow is unrealistic, given the nature of relations between the NATO allies and the American nuclear guarantees in NATO.



There is also the obvious need to include other nuclear-weapon states in any future NSNW dialogue. A serious agreement in this area will hardly be possible without taking into account those states' nuclear capability.

Apart from political differences, there are also several technical problems which must be resolved before any progress can be made on the NSNW front.

The experience of negotiations on strategic offensive reductions suggests that resolving technical issues (formulating precise definitions of the weapons being cut; developing verification mechanisms; agreeing the procedures for elimination or information exchange, etc.) requires much greater efforts than resolving headline strategic-level problems (ceilings, deadlines, phases, etc.). Over the past several decades Russia and the United States have accumulated a huge amount of definitions and legal instruments in the area of strategic offensive arms reductions, from precise terminology to a tried and tested system of inspections. No such definitions or instruments are available for non-strategic nuclear weapons talks, and the differences between NSNW and strategic offensive weapons are too great for the same verification mechanisms to be applicable.

Take, for example, the problem of defining strategic and non-strategic weapons. When the Soviet Union (Russia) and the United States worked on the text of the strategic reductions treaties, they proceeded from the notion that these treaties should cover all nuclear weapons systems capable of reaching the other country's territory. In other words, their understanding of what "strategic" means as applied to nuclear weapons only worked in a bilateral context; it cannot be used in dealings with the other nuclear-weapon states.

What is more, even Russia and the United States still have some unresolved differences concerning what kinds of weapons fall under the NSNW definition. For example, they do not agree on how to categorize long-range sea-launched cruise missiles. It is also well known that the same nuclear bombs can be deployed on strategic as well as non-strategic aircraft.

The problem of categories and definitions could be the starting point for NSNW discussions between the P5.

The delivery systems used for NSNW tend to be dual-purpose systems; they can be deployed with nuclear as well as conventional forces. Strategic offensive arms reductions have all been implemented by reducing the numbers of delivery systems. The same approach is unlikely to work in the case of NSNW. No country is likely to agree to eliminate delivery systems which can also be used for conventional weapons (i.e. aircraft, short-range missiles, surface-to-air missiles, torpedoes, weapons mounted on ships and submarines, and barrel artillery).

Essentially, NSNW reductions will have to be implemented by means of reduction and verifiable elimination of nuclear munitions—for which there has been no precedent in the history of negotiated nuclear disarmament.

In view of all the serious political differences and technical problems faced by any future NSNW limitation regime, there is understandable skepticism about the chances for signing a full-scale NSNW treaty containing verification measures any time soon. Even if the negotiations can be launched, they will be long and difficult. It is also obvious that any NSNW discussion can begin only if the parties manage to find solutions to the aforementioned strategic stability problems; these solutions are also required before any talks on further strategic offensive reductions can begin.

If and when the NSNW discussion begins—most importantly, in the P5 format—the most pressing objectives for such consultations would be as follows:

- reach an agreement on nuclear weapons definitions and classification;
- develop a mechanism for taking into account the impact of various types of weapons—including conventional weapons—on strategic stability;
- negotiate a commitment to remove all nuclear weapons stationed abroad back to national territory, and to ban any future deployment outside national territory;
- end the practice of military exercises and training events that involve the use of nuclear weapons by the armed forces of countries which do not possess such weapons;
- discuss the future of NSNW as part of a whole set of measures to limit other types of weapons, including conventional.

WHAT CAN NUCLEAR-WEAPONS COUNTRIES DO TOGETHER?

Until now, only two countries, Russia (the Soviet Union) and the United States, have participated in strategic offensive arms limitation talks. These talks began back in the late 1960s, and the two countries have signed a large number of bilateral agreements over the past decades.

The other official nuclear-weapon states, i.e. Britain, China, and France, are not taking part in strategic arms reduction talks. This is despite the fact that, in accordance with Article IV of the NPT, all of these countries have undertaken a commitment “to pursue negotiations in good faith on effective measures relating to cessation of the nuclear arms race at an early date and to nuclear disarmament. . . .”¹¹

Britain, China, and France justify their position by pointing out that their nuclear arsenals are much smaller than the Russian or U.S. stockpiles.

It is true that Russia and the United States account for the vast majority of strategic delivery systems and nuclear munitions in the combined arsenals of the P5.

Various sources estimate Britain’s nuclear arsenal at 180–225 warheads, France’s at 300–320 warheads, and China’s at 200–250 warheads (plus up to 150 non-strategic nuclear weapons).¹²

In talking about the future of the British, French, and Chinese nuclear arsenals, the following considerations must be kept in mind.

As far as Britain and France are concerned, it is safe to assume that, at the very least, neither country intends to increase its nuclear weapons stockpiles. There is, however, a lot of uncertainty about China’s plans.

In any event, and regardless of the various scenarios for the Chinese strategic nuclear arsenal, it is in Russia’s national interests to secure the involvement of Britain, China, and France in a multilateral dialogue on strategic offensive weapons.

This has been reflected in the Russian National Security Strategy,¹³ which states that:

- Russia is ready for further discussion of nuclear reductions based on bilateral agreements as well as multilateral formats.
- Russia will work to encourage the involvement of other countries, especially those which possess nuclear weapons, in the process of strengthening strategic stability.

The question of multilateral talks between all the countries which possess strategic offensive weapons has been raised on several occasions at the UN General Assembly, the UN Commission for Disarmament, the NPT review conferences, and other disarmament forums.

But for now, and despite the commitments undertaken in the NPT, there is no evidence that Britain, China, and France are willing to join the U.S.–Russian disarmament process. The three countries continue to claim that even after Russia and the United States have implemented the reductions mandated by the New START treaty, they will have to press ahead with further reductions on a bilateral basis.


It is important to stress that the strategic arms reduction process cannot remain bilateral indefinitely. Even at this stage Britain, France, and China can make their contribution. To begin with, they could undertake a commitment not to increase their nuclear arsenals.

One of the reasons for engaging the other nuclear powers in the strategic arms reduction talks would be to agree joint transparency measures, with joint verification measures to follow later on.

It appears that for now the other nuclear countries are only just beginning to look at the possibility of joint measures in the area of nuclear disarmament. At the 2010 NPT Review Conference, Britain, France, and China were categorically opposed to the idea that they should join the U.S.–Russian nuclear disarmament talks. They only agreed to go as far as hold some informal consultations on individual topics related to nuclear disarmament. There have already been several joint meetings to discuss the disarmament experience, nuclear weapons terms and definitions, and other issues pertaining to Article VI of the NPT. But none of the three countries has expressed any willingness to take concrete joint steps on nuclear disarmament.



In the longer term, the future multilateral regime should include not only the five official nuclear-weapon states, but every country which has serious nuclear weapons capability. The present author deliberately avoids using the term “de facto nuclear-weapon states,” lest such phrasing be taken by those countries as recognition of their nuclear status or equal standing with the NPT nuclear-weapon states. The author firmly believes that granting these countries recognition as official nuclear-weapon states would have a destructive impact on the NPT and is therefore completely unacceptable under any circumstances.

There is no doubt that the countries which possess nuclear weapons play an important role in the global balance of power. In a world dominated by two super-powers, the United States and Soviet Union, those two superpowers agreed to set up a bilateral strategic arms control regime. A new world with many centers of power requires a similar multilateral regime. 

For more analytics on disarmament, please, visit the section “Ways towards Nuclear Disarmament” of the PIR Center website: disarmament.eng.pircenter.org

NOTES

¹ Third Session of the Bilateral Consultative Commission under the New START Treaty, Russian Foreign Ministry, February 8, 2012, <http://www.mid.ru/brp_4.nsf/newsline/3F533672651420034425799E00510BA9>, last accessed January 22, 2013.

² Joint U.S.–Russian Statement on the Treaty on the Elimination of Intermediate-Range and Shorter-Range Missiles at the 62nd Session of the UN General Assembly, New York, October 25, 2007, United Nations, <http://www.un.int/russia/new/MainRootrus/docs/off_news/281007/newru2.htm>, last accessed January 22, 2013.

³ Joint Statement by Dmitry A. Medvedev, President of the Russian Federation, and Barack Obama, President of the United States of America, Regarding Negotiations on Further Reductions in Strategic Offensive Arms, London, April 1, 2009, <http://news.kremlin.ru/ref_notes/167>, last accessed January 22, 2013.

⁴ Joint Statement on the Parameters of Future Nuclear Arms Reductions, March 21, 1997, Helsinki, Electronic Fund of Acts of Legislation, <<http://docs.kodeks.ru/document/901857459>>, last accessed January 22, 2013.

⁵ *Nuclear Posture Review Report* (Washington, D.C.: Department of Defense, April 2010), <<http://www.defense.gov/npr/docs/2010%20Nuclear%20Posture%20Review%20Report.pdf>>, last accessed January 22, 2013.

⁶ *Active Engagement, Modern Defense: Strategic Concept for the Defense and Security of the Members of the North Atlantic Treaty Organization*. Adopted by heads of state and government at the NATO summit in Lisbon, November, 19–20, 2010 (Brussels: NATO, 2010).

⁷ General Assembly Fifty-seventh Session, *Official Records: 57th Plenary Meeting*, November 22, 2002, 10 a.m. (New York: UN), pp.7–8, <<http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N02/705/84/PDF/N0270584.pdf?OpenElement>>, last accessed January 22, 2013).

⁸ “On Russian Policy Regarding Arms Limitation and Reduction,” statement by Russian President Boris Yeltsin, January 29, 1992, *Rossiyskaya Gazeta*, January 30, 1992.

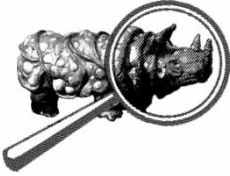
⁹ H. Cartland [et al.]; chair. W.J. Perry; vice-chair. J.R. Schlesinger. *America’s Strategic Posture: The Final Report of the Congressional Commission on the Strategic Posture of the United States* (Washington, D.C.: United States Institute of Peace Press, 2009), p. XVI.

¹⁰ *Deterrence and Defense Posture Review*, NATO, May 20, 2012, <http://www.nato.int/cps/en/natolive/official_texts_87597.htm?mode=pressrelease>, last accessed January 22, 2013.

¹¹ *Nuclear Weapons Non-Proliferation Treaty, Approved by Resolution 2373 (XXII) of the United Nations General Assembly on June 12, 1968*, United Nations, <http://www.un.org/ru/documents/decl_conv/conventions/npt.shtml>, last accessed January 22, 2013.

¹² See, for example: V.A. Dronov et al., *Nuclear Weapons of Britain, France, and China* (Moscow: Rosatom Institute of Strategic Stability, 2012), pp. 38, 77, 112.

¹³ *Russian National Security Strategy up to 2020*. Approved by Presidential Decree No 537 of May 12, 2009, Russian Federation National Security Council, <<http://www.scrf.gov.ru/documents/99.html>>, last accessed January 22, 2013.



Viktor Murogov

NUCLEAR ENERGY: LESSONS FROM THE PAST, CURRENT PROBLEMS, AND NEW INITIATIVES

Analysts offer all kinds of scenarios and projections for the future of global energy. But some key points in these projections are immutable: population growth; rising global energy demand; fierce competition for limited and unevenly distributed fossil fuel resources; growing dependence on unstable energy exporting countries; rising environmental concerns; a closing gap in energy consumption between the richest and the poorest countries; a limited and location-specific potential of alternative energy sources; and growing negative consequences of energy shortages brought on by population growth and other factors.

WHAT IS THE FUTURE OF NUCLEAR ENERGY?

In such circumstances, the role of nuclear energy—as the only new industrial-scale energy source capable of answering all these challenges—is undoubtedly set to grow. The volatility of the fossil fuel market (and the oil market, first and foremost), as well as the latest financial crisis, only serves to emphasize the importance of nuclear energy.

For many countries, especially the United States, nuclear technologies are not merely an element of the energy market. Perhaps even more importantly, they are the foundation of our economic, energy, and political security. They are also the basis of our social development in such areas as:

- nuclear medicine (new diagnostic and treatment methods for heart disease, cancer, etc.);
- food production and distribution (including safe new techniques of food storage);
- industrial quality control methods;
- nuclear-physics technologies, instruments and products (such as lasers, accelerators, and isotopes).

For Russia, nuclear technologies are a powerful instrument for building a high-tech economy, and for ending dependence on exports of raw materials by developing high-tech industries, with a key role played by education, the environment, and a safety culture as new engines of social and economic growth. Nuclear technologies are capable of delivering a five-fold increase in the proportion of machine-building and high-tech sectors in the structure of the Russian economy.

Speaking at the UN Millennium Summit in 2000, the Russian president proposed an initiative which highlighted nuclear technologies as the basis of energy security and sustainable development. The initiative was very timely, and it found a lot of support among the international community.

The initiative was also backed by several resolutions of the IAEA General Conference, which issued a recommendation to use it as the core of the INPRO international project involving 30 countries, and made it part of the agency's regular program.¹



The UN General Assembly also welcomed the Russian presidential initiative in its resolutions, describing it as an answer to the aspirations of the developing countries and as a way of harmonizing relations between the industrialized and the developing world.² But the actual implementation of that initiative (including as part of the INPRO project³) and analysis of the possible scenarios for nuclear energy development have demonstrated that nuclear energy and nuclear technologies themselves still require substantial improvement and innovation.

Following the accident at the Fukushima nuclear power plant in Japan the international community has been discussing a broad range of issues, from the future of the nuclear energy renaissance to the need for a new global regime of not only nonproliferation but also nuclear and radiation safety and security. Experts and decision-makers are discussing the need to set up new bodies, develop innovative governance methods, and implement compulsory new international standards.⁴

But these discussions often ignore the fact that the nuclear technologies in use today are 20 to 30 years old; that includes light water reactors, i.e. the VVER, PWR, and BWR reactor designs, as well as fast neutron reactors. More than 80 percent of the world's nuclear power plants rely on water-cooled and water-moderated thermal neutron reactors. That, in fact, is one of the key reasons for the stagnation of the nuclear energy industry in the leading Western countries.

Figure 1 illustrates why the current generation of nuclear technologies cannot underpin future growth. These technologies are completely reliant on U-235. The global reserves of that uranium isotope are actually an order of magnitude smaller than the reserves of oil and gas. How, then, can we expect nuclear energy based on such technologies to have any long-term future, or any stabilizing role?

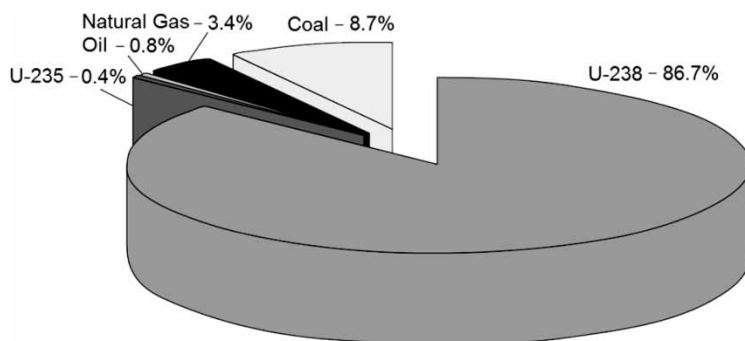
Another major problem is that at this point nuclear energy is used only for industrial-scale electricity generation. But the bulk of the natural energy resources (i.e. fossil fuels) are actually being consumed by such applications as industrial heating, central heating, and transport, where nuclear energy currently plays a marginal role.

More than 60 years since it was developed, high-temperature gas-cooled reactor technology (HTGR) still remains underutilized; only a few research and semi-industrial reactors have ever been built. Such reactors were at one point expected to become the basis of a nuclear-hydrogen energy industry by generating synthetic liquid fuel. That would enable nuclear energy to be used in transport and industrial heating (800°C and above) applications.⁵

Another technology which is not being utilized is nuclear-powered central heating plants. Russia began to build such plants in Nizhny Novgorod and Voronezh, but then abandoned the projects.

Yet another technology that could be put to a much better use is small energy reactors (with an output of less than 100 MWe), which could be very attractive for the developing countries and as an autonomous power source in off-grid locations. In Russia, for example, only 12 percent of the territory is covered by the electricity grid and suitable for large nuclear power plants (1,000 MWe

Figure 1. Relative Energy Content of Natural Fuel Sources (Energy), Not Counting Renewables



Source: *Nuclear Technology Review 2006*, “Key Issues” (Vienna: IAEA 2006), pp. 12–20.

and above). Very promising designs have been proposed by foreign and Russian engineers (4S in Japan, PRISM in the United States, SVBR in Russia, etc.)—but none of them has been commercialized. That is especially surprising in the case of the United States and Russia (Soviet Union), which have accumulated vast experience in this area, having built about 1,000 small reactors for nuclear-powered submarines.⁶

The key problem of sustainable development is the problem of utilizing the reserves of natural uranium and thorium for nuclear energy. It is important to stress that solutions here can be found. These solutions require innovative new technologies, and a new technology platform. Let us therefore look at these technologies in greater detail, because the existing technological approaches not only fail to address the problems of future sustainable development of nuclear energy, but can actually pose additional obstacles.

INNOVATIVE TECHNOLOGIES AND PROLIFERATION RISKS

A radical solution, a solution that has already been validated by experiments and semi-industrial scale application, has actually been available for a long time. Back in 1944 Enrico Fermi proved the possibility of utilizing the reserves of natural uranium and thorium (which are almost unlimited) by using fast-neutron reactors in a closed nuclear fuel cycle (NFC).⁷ In this day and age it is almost undisputed that full-scale development of nuclear energy as a basis of sustainable growth can be achieved only by using a closed nuclear fuel cycle and fast breeder reactors.⁸ That is precisely the global objective now being pursued by leading international projects such as INPRO (launched on Russia's initiative in the IAEA framework) and GIF IV (the fourth-generation reactor project spearheaded by the United States and involving only the leading nuclear countries).

The task has turned out to be much more complex technologically and politically than the nuclear energy pioneers had envisaged. To understand why, let us look at the background of the fast reactor technology.

Research into fast neutron reactors has been under way for more than six decades. In 1944 Fermi proposed the original concept of fast reactors. In 1946 the United States launched the first experimental fast reactor, codenamed Clementine, which worked on plutonium and used mercury as the coolant.⁹ In 1951 the EBR-1 experimental breeding reactor in the United States generated the first nuclear electricity.¹⁰

The EBR-II was the world's first reactor to utilize a closed nuclear fuel cycle; the project was conducted in 1964–1968. The reactor used metallic fuel and liquid metal as coolant. The JFR nuclear fuel cycle involved metallic vapor processing and recycling of actinides (uranium, plutonium, etc.) from spent fuel.¹¹

In the Soviet Union research into fast reactor technologies began in 1949; the project was led by Alexander Leypunsky. In 1956 the Soviet Union launched the BR-2 experimental breeder reactor, which was similar to the Clementine. Then in 1959 it was replaced by the BR-5 (built at the FEI institute in Obninsk), which had a thermal power output of 5 MW. The BR-5 was the prototype of the future BN-type reactors (oxide fuel, cooled by liquid sodium). In 1973 the Soviet Union launched the world's first semi-commercial BN-350 reactor in Kazakhstan, and in 1980 the BN-600 reactor at Beloyarskaya NPP. The BN-600 is currently the world's only operational fast-neutron energy reactor. Nevertheless, Russia has never been able to implement a closed uranium–plutonium nuclear fuel cycle. The BN-type reactors (BN-350 and BN-600) have always worked in an operational mode which consumes uranium (enriched to more than 20 percent) rather than breeder mode.

Development of a new type of reactor with liquid-metal coolant had taken a lot of research and efforts by three or four generations of scientists. But even in those countries which have developed such technology (such as the United States) the fast reactor and closed NFC know-how and expertise have largely been lost. It has now become obvious that this was a policy mistake by the United States, which shut down almost all of its fast reactors and closed NFC programs in the 1970s.¹²

That loss of know-how and expertise was not merely an economic loss, and a waste of tens of billions of dollars. It was in fact a real science and technology catastrophe; an entire branch of research was allowed to fall apart, and leadership in the area of important nuclear energy technologies was lost. The losses include:



- ❑ professional and highly trained specialists;
- ❑ a system of higher education in the relevant area, including professors and researchers;
- ❑ experimental facilities and laboratories;
- ❑ new generations of young scientists.

Rebuilding the things which have been allowed to crumble will take decades of energetic efforts, and may in fact prove impossible.

The main obstacle on the way to rebuilding these branches of research and developing an innovative technology platform for nuclear energy development is the need to train a new generation of specialists. Such training programs should always be several steps ahead of the actual research programs and projects to build nuclear energy facilities. Launching new nuclear power plants (NPPs) and other nuclear facilities is simply dangerous unless there is an adequate personnel training policy in place.¹³

GLOBAL NATURE OF NUCLEAR TECHNOLOGIES AND NATIONAL SOVEREIGNTY

The international community—including the IAEA, other international nuclear organizations, and national nuclear laboratories—has learned important lessons about radiation and nuclear safety and security, environmental problems, and other aspects of nuclear energy development. That experience has been reviewed and analyzed once again following the accident at the Fukushima NPP. There are good reasons to believe that the bulk of these problems can be resolved by new technologies and engineering solutions.

The only major problem which cannot be resolved through technology alone, and which requires political solutions, is the problem of nuclear nonproliferation. There is a serious conflict between the global nature of nuclear technologies (a nuclear accident always has global repercussions) and the national nature of responsibility and control; in other words, national sovereignty often gets in the way of resolving global problems. In some sense, the proliferation problem is only going to get even worse as innovative technologies continue to make progress. New fast breeder reactors, reprocessing and recycling of fissile materials, transmutation, large numbers of small NPPs, increasing numbers of nuclear specialists, a growing need for transportation of nuclear materials, and other factors (see Tables 1 and 2) will increase the risk of proliferation of sensitive nuclear expertise, materials, and equipment.

SCIENCE, TECHNICAL AND POLITICAL COOPERATION

When nuclear energy and nuclear weapons research was still in the early stages, luminaries such as Fermi, Szilard, and Einstein were already warning about the global consequences of that

Table 1. Proliferation Risk Factors

Growth of the nuclear energy industry	
1	Growing numbers of nuclear power plants, including small regional NPPs
2	Growing numbers of nuclear fuel cycle facilities
3	Growing need for transportation of nuclear materials
4	More nuclear waste
Structural changes in the nuclear energy industry	
1	Nuclear fuel breeding, use of fast breeder reactors
2	Spent nuclear fuel reprocessing and recycling, closed nuclear fuel cycle
Growth of the nuclear energy industry in newcomer countries which do not have the necessary expertise to ensure proper nuclear security, safety, and nonproliferation standards	

Source: *Nuclear Technology Review 2006* “Key Issues” (Vienna: IAEA, 2006), pp. 12–20.

Table 2. Ways to Boost the Resilience of the Nonproliferation Regime

Changes in the nuclear industry can lead to greater availability and accessibility of nuclear materials and technologies, thereby increasing proliferation risks

New approaches and measures are required to keep those risks from getting worse, at the very least	
Measures that are necessary in all areas which underpin the regime	Political Institutional Technical
Systemic analysis and quantitative assessment of the proliferation risks are required to address these problems	

Source: *Nuclear Technology Review 2006*, “Key Issues” (Vienna: IAEA, 2006), pp. 12–20.

research. They predicted that nuclear energy would play a key role in the future—but they also warned of the need for a reliable international system of nuclear safety and security. What they had in mind was not merely technologies enabling safe use of nuclear energy, but also a security regime to prevent a runaway proliferation of nuclear technologies and to place them under international controls.¹⁴

One of the key initiatives in this area was the Atoms for Peace program initiated at the United Nations by U.S. President Dwight Eisenhower in 1953. The initiative quickly garnered broad international support, and in 1954 the UN General Assembly adopted a resolution which backed the program. One of its key elements was the decision to establish the International Atomic Energy Agency (IAEA).

The IAEA Statute was approved in 1956, and the organization itself was set up the following year. In 1955 Geneva hosted the first international conference on the peaceful use of nuclear energy. Similar events attended by renowned nuclear scientists were held in 1958, 1964, and 1971. These events launched practical international cooperation on the peaceful use of nuclear energy.

A key factor in further development of peaceful use was the entry into force in 1970 of the Nuclear Non-Proliferation Treaty. At about the same time several regional organizations were set up to consolidate national efforts and to provide additional guarantees of peaceful and effective development of nuclear science and technology. These organizations include the Nuclear Energy Agency and the International Energy Agency in the OECD countries, Euratom in the European Union, etc.

The global nature of the development of nuclear technologies was also reflected in the creation of several specialized international organizations, including the World Association of Nuclear Operators (WANO); the World Nuclear Association (WNA), which brings together nuclear industry companies and organizations; the World Nuclear University (WNU); and several others. Another element of the same trend is the Kyoto Protocol, which also reflects the global nature of the world’s energy problems.

INTERNATIONALIZATION OF THE DEVELOPMENT OF NUCLEAR TECHNOLOGIES

The establishment and development of global (multinational) nuclear energy organizations was happening in parallel with the realization of the key role of nuclear fuel cycle technologies in resolving the nonproliferation problem. In the 1970s–1980s the world began to discuss various ideas, concepts, and proposals on international integration of the nuclear fuel cycle (one notable event was a workshop in Salzburg in 1977¹⁵). The ideas included:

- creating regional NFC centers;
- establishing international centers for handling spent nuclear fuel and plutonium.

An important stage in the discussion of various NFC concepts was the international nuclear fuel cycle assessment conducted in 1978–1980 with active participation of experts from 18 leading



A N A L Y S I S

countries. But for various political and economic reasons—including the great political and economic importance of nuclear technologies for the economies of many countries—until the end of the twentieth century those discussions and proposals remained on paper.¹⁶

INTERNATIONAL NFC CONCEPT: THE CURRENT STATE

Several very important initiatives were put forward at the turn of the twenty-first century to bolster international cooperation in the area of nuclear technologies, which are seen as the basis of sustainable energy development. These include the initiative proposed by Russian President Vladimir Putin at the UN Millennium Summit in 2000; and the U.S. initiative which has resulted in the establishment of the GIF IV International Forum. The latter aims to develop innovative fourth-generation reactor technology and a nuclear fuel cycle. These initiatives came as a harbinger of a more mature approach to nuclear energy development, which takes into account the mistakes and lessons learnt in the previous years—including the lessons of Three Miles Island, Chernobyl, etc. That has required meticulous analysis of all the positive and, most importantly, negative experiences.

The following things have become absolutely clear to experts and specialists:

- ❑ Future sustainable economic growth and energy security on a global scale, taking into account the needs of the developing countries (especially China, India, Brazil, Argentina, etc.) are impossible without nuclear energy. In addition to power generation, nuclear energy has other important applications in healthcare, food and water supply, science, technology, and industry, etc.
- ❑ There are technological solutions available for such key nuclear energy problems as safety and security of nuclear power plants and nuclear fuel cycle facilities—including the problem of spent nuclear fuel management and nuclear waste disposal. The important thing is to secure sufficient financial, material, and human (intellectual) resources.

Further nuclear energy development is facing only one major challenge for which no obvious solutions have been proposed: the problem of nuclear nonproliferation. This is a complex technological and political problem consisting of three individual components, each requiring its own solution:

- ❑ accounting of fissile materials (part of the IAEA remit);
- ❑ technological and design barriers to proliferation;
- ❑ measures such as international agreements, conventions, and other solutions.

The world has also come to the realization that almost every step in the development of NFC technologies can also be viewed as a potential step towards military use of nuclear technologies. The focus has therefore shifted to the question of how to make use of the benefits of nuclear energy without the risk of proliferation of NFC technologies (especially enrichment, production of highly enriched uranium, spent fuel reprocessing, and the use of plutonium fuel). In 2003 a group of experts from leading nuclear countries published an IAEA-commissioned report “Multilateral Approaches to the Nuclear Fuel Cycle” (INFCIRC/640). In 2004 the World Nuclear Association published another report, headlined “Ensuring Security of Supply in the International Nuclear Fuel Cycle.” Several individual countries (the United States, Russia, Japan, Germany, and others) have also proposed various national initiatives in this area. The following three initiatives are probably the most comprehensive:

- ❑ international NFC centers for nuclear fuel enrichment and spent nuclear fuel processing (Russia);
- ❑ international nuclear fuel banks for assured access to NFC products and services (Russia, Germany, the WNA, and others);
- ❑ the Global Nuclear Energy Partnership (GNEP), proposed by the United States and supported by more than 20 countries.

The obvious question is, how can we make sure that these latest initiatives do not remain on paper—which is exactly what has happened to all the earlier initiatives? How can we overcome the

passive or even hostile attitude to these initiatives by several countries which see them as discriminatory—even though their proponents say the objective is to help the developing nations in peaceful use of nuclear energy?

EFFECTIVE DEVELOPMENT OF NUCLEAR ENERGY

Let us briefly summarize the problems facing nuclear energy technologies as a solution to the world's energy problems. It has now become obvious that the task of developing nuclear weapons has proved easier to accomplish than the task of developing modern nuclear energy reactors and nuclear fuel cycles. It will be impossible to make the best possible use of nuclear energy without commercializing the breeder reactor technology with a closed NFC.

Of the six types of future nuclear reactors selected for the GIF IV international project, four are fast-neutron reactors. Three of them use liquid metal (sodium, lead, or lead–bismuth alloy) and one uses gas (helium) as the core coolant.

Development of the breeder reactor technology (including fast reactors using the uranium–plutonium NFC and slow neutron reactors using the thorium NFC) has been ongoing for over 60 years. In 1968 the United States launched the MSBR thorium-cycle molten-salt breeder reactor at the Oak Ridge National Laboratory. The reactor, which had a breeding ratio of more than one (1.06),¹⁷ remained in operation for seven years.

For more analytics on international nuclear energy cooperation, please, visit the “Development of Russia’s Nuclear Exports” project section of the PIR Center website at: atom.eng.pircenter.org

Experiments conducted using the world's first semi-commercial fast-neutron reactor, the BN-350 (Kazakhstan, Soviet Union) achieved a breeding ratio of 1.3 for the plutonium fuel cycle. A French fast-neutron reactor has achieved an industrial-scale closed NFC with repeated fuel recycling and a breeding ratio of 1.2–1.3.¹⁸ The Beloyarskaya NPP in Russia, which operates the BN-600 fast-neutron reactor, has been working reliably since 1980; an upgraded BN-800 version of the reactor is now under construction. None of the BN-type reactors, however, is currently being operated in the fuel breeder mode.

There is still no single concept (or demonstration) of a commercial fast energy reactor with a closed NFC. Development of innovative new NPPs (fast reactors, as well as high-temperature gas-graphite reactors for nuclear-hydrogen applications, or supercritical PWR reactors), which is one of the objectives of the INPRO and GIF VI international projects, has turned out to be too complex and expensive for any single country (even such leaders as the United States, the former Soviet Union, France, Japan, etc.). In actual fact, financing is not the biggest problem. Serious nuclear accidents, including the recent accident at the Fukushima NPP in Japan, have demonstrated that there is no more room for mistakes. Specialists agree that another serious nuclear accident would spell the end of nuclear energy.

Development and implementation of fast reactor projects with a closed NFC has proved too great a task for a single generation of researchers and engineers. It has also become clear that this task requires the kind of technological expertise which only a very limited number of countries possess (including France, Russia, Japan, and India). Re-building lost expertise in this area is one of the main objectives of the U.S.-sponsored GIF initiative, which aims to develop fast reactors with a closed NFC.

Developing a commercially viable fast reactor with a closed NFC is not, however, the only task that must be accomplished to facilitate the development of nuclear energy. There is also the problem of dealing with highly radioactive waste, which must be addressed at the regional level at the very least because it is so complex, expensive, and dependent on specific conditions in some countries (such as the densely populated Western European or Southeast Asian nations).

Another related problem is the need to develop and commercialize the technology for transmutation of long-lived fission products and disposal of actinides generated by fast reactors. A similar solution is also required for the thorium fuel cycle.



Effective solutions to these global problems are impossible without international cooperation. They require the pooling of financial, material, and, most importantly, intellectual resources of the countries which have the necessary expertise, technological capability, and industrial infrastructure.

In order to achieve a consensus in addressing the problem of nonproliferation, as well as NFC security and safety, proponents of multilateral nuclear energy initiatives must demonstrate how the developing and small countries (such as the Eastern and Central European nations) can benefit from these initiatives in the long term, and not just in the immediate future. We must not delay studying, discussing, and demonstrating the need for cooperative solutions to nuclear energy problems based on such initiatives as the International NFC Centers and the Global Nuclear Energy Partnership. This includes the need to establish and develop:


- NFC enrichment centers (which is something Russia has already proposed) to provide the developing and small countries with low-enriched uranium fuel;
- NFC spent nuclear fuel removal centers (the proposal is currently being discussed);
- NFC centers specializing in processing spent nuclear fuel and extracting plutonium from it;
- NFC centers specializing in producing plutonium fuel for fast reactors and in utilizing that fuel in fast-neutron reactors;
- NFC centers specializing in the production of U-233 in fast reactors (with thorium screens) and using that uranium to make low-enriched (synthetic) fuel for thermal reactors: U-233 + U-238 (for long-term provision of fuel to developing and small countries);
- NFC centers specializing in nuclear waste disposal.

Obviously, some NFC centers can specialize in more than one of these six areas; for example, removal of spent nuclear fuel can be combined with spent fuel processing and extraction of plutonium. A comprehensive solution to all these problems can only be found through international cooperation because it requires enormous financial, material, and human resources. No country can do it on its own.

The goals and objectives outlined in this paper are truly a global goal of the century. Unless these goals are achieved, we may see the spread of sensitive nuclear technologies, including enrichment and spent fuel reprocessing, with potentially a dozen new countries acquiring nuclear weapons by the middle of this century. The small and developing countries must see the need for and the benefits of the multilateral nuclear initiatives; they must understand what changes they must make in their national programs, and clearly see all the upsides and downsides of participation.

Such an approach will also require research and analysis in the following areas:

- analysis of the requirements for the infrastructure of the states taking part in multilateral initiatives (in areas such as education, controls in the knowledge transfer system, regulating bodies, engineering and technological infrastructure, etc.);
- analysis of the program for managing and preserving nuclear know-how under the IAEA's auspices to ensure that knowledge and experience are passed on to the next generations of specialists (this is a separate problem in which the IAEA must play a leading role) and to new developing countries.

Successful implementation of these initiatives will be instrumental for ushering in a new era of nuclear energy development, sometimes described as a nuclear renaissance. 

NOTES

¹ *Multilateral Approaches to the Nuclear Fuel Cycle*, Expert Group Report to the DG IAEA (Vienna, 2005).

² R.M. Timerbaev, *International Controls over Nuclear Energy* (Moscow: PIR Center, 2003).

³ *Multilateral Approaches to the Nuclear Fuel Cycle. Regional Nuclear Fuel Cycle Centers*. Report of the IAEA Study Project (IAEA, 1977).

⁴ *International Nuclear Fuel Cycle Evaluation*, IAEA, Vol. 9: Summary Volume, STI/PUB/534/1980 (Washington, D.C., Oct. 1977).

⁵ V.M. Murogov, N.N. Ponomarev-Stepnoy, et al., "IAEA International Initiatives: From Innovative Nuclear Technologies to Increasing the Role of Nuclear Education," *Bulleten po atomnoy energii* No. 6 (2007), pp. 37–41. T.E. Shea, V.S. Kagramanian, et al., "Proliferation Resistance in Innovative Nuclear Reactors and Fuel Cycles," 10th International Conference on Nuclear Engineering, April 14–18, 2002.

⁶ IAEA, "International Nuclear Fuel Cycle Evaluation (INFCE)," February 1980. H. Feiveson, "The Search for Proliferation Resistance of Global Civilian Nuclear Power Systems (TOPs)," report by the TOPs Task Force of the United States Department of Energy, Nuclear Energy Research Advisory Committee, January 2001.

⁷ International Topical Workshop on Proliferation Resistance in Innovative Reactors and Fuel Cycles, International Atomic Energy and Landau Network, Centro Volta, Como, Italy. 2001.

⁸ V. Khlebnikov, "The Role of the IAEA in resolving Pressing Problems of Nuclear Weapons Nonproliferation," *Yaderny Kontrol* No. 1 (71, 2005), pp. 81–96.

⁹ Y.A. Korovin and V.M. Murogov, *Breeder Reactors in Tomorrow's Nuclear Energy* (Obninsk: IATE, 1990).

¹⁰ G.M. Pshakin, N.I. Geraskin and V.A. Apse, *Nuclear Nonproliferation* (Moscow: MIFI, 2004).

¹¹ "The Future of Nuclear Power," an interdisciplinary MIT Study, 2003.

¹² IAEA, "International Nuclear Fuel Cycle Evaluation," IAEA Working Group Reports, 1980.

¹³ IAEA, *Guidance for the Application of an Assessment Methodology for Innovative Nuclear Energy Systems* (Vols. 1–7), IAEA-TECDOC-CD 1575 (Vienna: IAEA, in preparation).

¹⁴ *Ibid.*; *Methodology for the Assessment of Innovative Nuclear Reactors and Fuel Cycles: Report of Phase 1B of INPRO*, IAEA-TECDOC-1434 (Vienna: IAEA, 2004); *Guidance for the Evaluation of Innovative Nuclear Reactors and Fuel Cycles: Report of Phase 1A of INPRO*, IAEA-TECDOC-1362 (Vienna: IAEA, 2003).

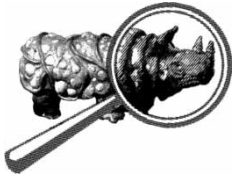
¹⁵ Khlebnikov, op. cit.

¹⁶ V.M. Murogov "The Training of Specialists and the Future of the Nuclear Industry," *Bulleten po atomnoy energii* No. 10 (2006), pp. 46–48.

¹⁷ *Nuclear Technology Review* (2006), pp. 12–20. S. Guindon, "History and Status of the Generation 4 International Forum," IAEA-CN-108-72, 2003.

¹⁸ Korovin and Murogov, op. cit. *Fast Reactor Database: 2006 Update*, IAEA-TECDOC-1531 (Vienna: IAEA, 2006).





Elena Zinovyeva

U.S. DIGITAL DIPLOMACY: IMPACT ON INTERNATIONAL SECURITY AND OPPORTUNITIES FOR RUSSIA

The term *digital diplomacy*, which has recently gained popularity along with such terms as *Internet diplomacy*, *social networks diplomacy*, and *Web 2.0 diplomacy*, was initially used in the context of U.S. foreign policy. It denoted broad use of information and telecommunication technologies (IT), including the *new media*, social networks, blogs, and other media platforms on the Internet.¹ At present, several other countries besides the United States are pursuing digital diplomacy programs. A case in point is the NATO countries, which are currently considering their own digital diplomacy programs.²

EVOLUTION OF THE TERM AND ITS LEGAL FRAMEWORK

The U.S. government defines digital diplomacy as the use of social networks in U.S. diplomacy in order to facilitate the interaction between American diplomats and Internet users in other countries.³ Washington's digital diplomacy is one of the branches of public diplomacy which aims to engage broad sections of society as opposed to the political and diplomatic elite in foreign countries. According to the Russian researcher Natalia Tsvetkova, the instruments of "Web 2.0 public diplomacy" include "making radio and TV programs available on the Internet, facilitating free access to literature about the United States in a digital format, monitoring discussions in the blogosphere, creating personal pages of U.S. government members in social networks, and distributing information via mobile phones."⁴

The United States is implementing its digital diplomacy programs with the help of large IT companies, including such heavyweights as Google. The Department of State's efforts in the digital domain have been spurred by the realization of the Internet's power to influence large numbers of PC and mobile phone users around the world. More than 30 percent of our planet's population are active Internet users, and the figure continues to grow every year.⁵

To understand the nature of digital diplomacy, it is important to understand that such diplomacy is a technological instrument. U.S. foreign policy and digital diplomacy are based on ideological foundations which are being effectively promulgated through the business model and information policy of Google, Facebook, Twitter, and other American IT companies. At the core of these ideological foundations are democracy and liberal values. The philosophical background of digital diplomacy is explained in various papers by Anne-Marie Slaughter, who served as the Director of Policy Planning at the Department of State in 2009–2011. In Dr. Slaughter's opinion, the countries that are the most "networked" in terms of information and communication channels are the ones which set the global agenda.⁶

The first American digital diplomacy programs were initiated in 2002–2003, when the George W. Bush administration began to make the traditional radio and TV channels broadcasting to the international audience available on the Internet. In 2006 the then Secretary of State, Condoleezza Rice, formed the Digital Outreach Team, which included specialists monitoring the flows of information and deliberate misinformation about the United States generated by users of social networks. She then announced the launch of the Department of State's first official blog. The U.S. government portal and several electronic journals were launched later that year.⁷



The next U.S. Secretary of State, Hillary Clinton, initiated a U.S. foreign policy refresher program dubbed “21st Century Statecraft”. Digital diplomacy was one of the key parts of that program. The Department of State’s initiative calls for an augmentation of the traditional foreign policy instruments with innovative instruments of state governance aimed at facilitating the realization of the full potential of networks, technologies, and populations in an interdependent world.⁸ Digital diplomacy programs reached a whole new political level under Hillary Clinton. They were tasked with achieving important U.S. foreign policy goals, such as discrediting the ideology of Al Qaida, the Taliban, and other anti-American movements, and undermining the political regimes in Iran, China, and several other countries by fomenting protest and fostering new dissident movements.⁹

At present, U.S. digital diplomacy programs are being implemented by several government agencies, including the Department of State, the CIA, the Department of Defense, and USAID. As of early 2012, coordination of public diplomacy on the Internet was the domain of Judith McHale, Under Secretary of State for Public Diplomacy. She was in charge of promoting American radio stations and TV channels targeting the international audience on the Internet. Her assistant for innovative technologies, Alec Ross, oversaw the social networks part of that effort.

In 2010–2011 the White House released several official papers setting out the priorities of digital diplomacy. One of those papers is headlined “Public Diplomacy: Strengthening U.S. Engagement with the World.”¹⁰ It outlines the goals which the U.S. government wants digital diplomacy to achieve:

- discredit the ideological enemies of the United States;
- counter China’s information campaigns on the Internet;
- limit Russia’s media presence in the former Soviet republics;
- counter Iran’s external cultural policy conducted via social networks.

Another task of digital diplomacy is to support youth movements. One of the greatest achievements in this area was a movement in Colombia organized with the help of Facebook. The movement soon turned into a wave of mass protests against the FARC rebels in 2008.¹¹ Shortly afterwards the United States initiated the establishment of the so-called Alliance of Youth Movements, which brings together young people who want to use new technologies for political purposes. The website of the Alliance offers instructions on how to set up a blog or launch a campaign in the social media.¹²

An important role in U.S. digital diplomacy in the Middle East belongs to the Digital Outreach Team, which was set up in 2006. The group’s tasks include participation in discussions about U.S. foreign policy on popular websites in Arabic, Farsi, and Urdu. Until the mid-1990s American public diplomacy efforts were spearheaded by the United States Information Agency, whose methods relied on one-way communication. After the start of the war in Iraq in 2003 the George W. Bush administration launched programs that aimed to use radio and television as public diplomacy instruments. But the audiences in the Middle East did not have much trust in such information sources. This highlighted the need for dialogue and interaction, which is why the Digital Outreach Team was set up. Supposedly, the Team’s mission is to explain U.S. foreign policy and counter misinformation campaigns.¹³

Several months after Hillary Clinton’s speech about freedom of the Internet, in May 2010 the White House unveiled the U.S. International Strategy for Cyberspace.¹⁴ In accordance with that strategy, defending human rights—especially freedom of information on the Internet—is one of the U.S. foreign policy priorities. In September 2010 the Department of State released a document headlined “IT Strategic Plan: Fiscal Year 2011–2013 Digital Diplomacy”.¹⁵ The paper specified and detailed the digital diplomacy objectives in the context of Washington’s foreign policy priorities. It said that one of those priorities was to strengthen international security and to form a positive image of the United States in other countries.

Other digital diplomacy priorities include:

- financing projects to develop and promulgate the spread of new technologies that allow users to circumvent censorship on the Internet;
- creating information services aimed at supporting the opposition in authoritarian countries;

- creating shadow Internet systems and independent mobile networks which, when deployed in third countries, can help the opponents of authoritarian regimes to exchange information online, circumventing the government's restrictions.¹⁶

The U.S. government has approved a number of documents which concern military-political aspects of the development of the Internet. In June 2011 it released parts of the Department of Defense Strategy for Operating in Cyber Space.¹⁷ The document views Cyber Space as a potential theater of combat action, along with land, sea, air space, and outer space.¹⁸ The DoD strategy is an extension of the National Security Strategy approved by the Obama administration in 2010.¹⁹ The strategy also views Cyber Space as a potential theater of combat action.

The U.S. foreign policy strategy in the global information sphere appears very coherent and aimed at furthering U.S. national interests. The objectives of digital diplomacy must therefore be viewed as complementary to the military-political objectives of maintaining U.S. leadership in the global information sphere. In his assessment of U.S. foreign policy in this area, the Russian expert Evgeny Rogovsky concludes that the overarching goal of that policy is global American leadership.²⁰

In 2011 the digital diplomacy programs attracted a lot of attention, especially in the wake of the mass protests in the Middle East and North Africa, dubbed Twitter-revolutions by the media. Experts have published several papers assessing the role of social networks and the new media in the so-called Arab Spring. Many Russian and foreign researchers believe that the young people were the driving force in all these protests; they have become a completely new political force, which currently does not have a clear ideological platform. The protests have also demonstrated the independent role being played by the media and the Internet. At the same time, some experts believe that social networks functioned merely as neutral communication channels and did not play any decisive role in the Arab Spring. It has also been argued that social networks served as a catalyst of the mass protests, but on a fundamental level those protests were caused by the social, economic, political, and religious situation in each individual country.²¹

Nevertheless, U.S. digital diplomacy has played an important role in directing and shaping the revolutions.²² The official position of the White House on the Arab Spring was formulated in an article by Alec Ross, Chief Advisor to Hillary Clinton. He believes that social networks played a coordinating role in the Middle Eastern revolutions, but that role was far from decisive.²³ He also comments, however, on the transforming role of IT in politics and diplomacy. He argues that IT is an important channel for ideas, and that it facilitates democratization and diffusion of power in domestic as well as foreign politics—although dictatorial and authoritarian regimes can also use IT for their own ends. Similar ideas have been voiced by Joseph Nye, a prominent U.S. political scientist, in his book “The Future of Power.”²⁴

A study conducted in August 2010 by the United States Institute of Peace suggests that the new media have the potential to change how citizens think or act, mitigate or exacerbate group conflicts, facilitate collective action, spur a backlash among regimes, and garner international attention toward a given country. At the same time, the authors of the study say that it is impossible to draw definitive conclusions concerning the effects of social networks on protests and revolutions in the Middle East and North Africa. The traditional media have retained the same or even a greater degree of influence compared with the social media.²⁵ Another study by the Dubai School of Government, headlined “Civil Moments: The Impact of Facebook and Twitter”, suggests that social networks, whose users are increasingly pursuing political goals, played an important role in mobilizing citizens and shaping public opinion. It points out that the number of Facebook users shot up by 30 percent in the first few months of 2011.²⁶ Researchers from Dubai reach a similar conclusion that the social media played an important but not decisive role in fomenting the mass protests and revolutions in North Africa and the Middle East. Scholars around the world are also offering different opinions regarding the role of the U.S. digital diplomacy programs as a catalyst of protest.

There is a broad range of attitudes to digital diplomacy in the U.S. expert community. Evgeny Morozov, a researcher at Georgetown University, highlights the dangers posed by the spread of social networks. He argues that the Web 2.0 services empower not only diplomats and pro-Western groups, but radical organizations as well.²⁷ He seems to have been vindicated by the outcome of the 2012 parliamentary elections in Egypt, in which representatives of the political wing of the Muslim Brotherhood, an Islamist organization, won the majority of the seats in the



lower chamber. Dr. Morozov also says that the Internet can not only serve as an effective instrument of democratization, but also strengthen authoritarian trends which restrict freedom.

Oxford University has also conducted studies of the effectiveness of digital diplomacy programs. The DoS Digital Outreach Team initiated a number of discussions on the Internet focusing on Barack Obama's Cairo speech in 2009. Analysis of the content of users' messages indicates that their reaction to these discussions was mostly negative, and that they clearly did not trust the message promulgated by the Americans.²⁸

Researchers point out that the U.S. public diplomacy initiatives in the Middle East were primarily dictated by fears for the international reputation of the United States after the 9/11 events, as well as national security concerns. In that context, the war of ideas was viewed as an integral component of the war on terror. Jamie Metz, an American researcher, makes a similar conclusion that the use of IT and satellite television as instruments of U.S. public diplomacy aims to "legitimize the use of force."²⁹

Having looked at the definition of digital diplomacy, its background and key characteristics, let us now look at the impact the U.S. programs in this area are having on international security.

IMPACTS ON INTERNATIONAL SECURITY

In the broadest possible sense, security is defined as an absence of threat. For a long time international security presupposed the absence of a major war, and the nature of threats was mostly military-political. The central problem was the so-called security dilemma, which emerges when a country becomes stronger, in an anarchic international environment that makes other countries worry for their own security. This results in an arms race, which perpetuates the cycle of conflict and, as a rule, leads to war. The situation changed in a significant way in the twentieth century following the arrival of nuclear weapons, which made a big war between superpowers impossible.

But in the late twentieth/early twenty-first century the international security environment underwent another significant change. According to Vladimir Kulagin, a prominent Russian researcher, the definition of international security is becoming much broader.³⁰ In addition to the traditional state actors, we now have new actors in the international security arena, including terrorist networks, transnational crime syndicates, and private defense contractors. There are also new, non-military threats, such as the environmental, economic, and information threat. A distinctive characteristic of the information sphere is that non-state actors play a notable role here and affect the international security situation, with such new threats as cybercrime and cyberterrorism now prominently on the security agenda. It therefore seems obvious that the threats resulting from various digital diplomacy programs and initiatives must be considered in the general context of information security.

There is no consensus in the academic community about the use of the terms information security and cybersecurity. This stems from the different approaches of different countries to defining the IT-related threats which require international regulation.³¹ The provision of information security in the technical sense includes protection, control, and enforcement of laws and regulations in the telecommunications sphere. The definition includes protection from unauthorized access, hacking of computer networks and websites, logic bombs, computer viruses and malicious software, unauthorized use of spectrum, radio-electronic attacks, etc.

The provision of information security in the psychological sense includes protection of the psychological state of the society and country from any negative information impact. Russian researchers and diplomats tend to prefer the second, broader approach, whereas the United States, the EU states, and some other countries stick to the first approach. This study will use both terms, depending on the context. At the same time, the main threats related to the implementation of digital diplomacy programs lie outside the purely technological and software domain, so this study uses the broader approach to defining information security.

Information security became part of the international political agenda—and, therefore, of academic and public discourse – after the end of the Cold War; it was a consequence of the new geopolitical situation and the IT revolution. Initially the term information security was used in the IT context when discussing problems which affect computer systems. In later years the definition was expanded beyond the purely technological domain.

It is safe to say that the U.S. research community holds the lead in the research of cybersecurity problems. In particular, RAND Corporation analysts have developed a concept of second-generation information wars. In accordance with that concept, information attacks are seen as a new type of attacks in the framework of strategic rivalry. Russian researchers view information security in the context of the so-called triad of threats to international information security, which includes the terrorist, military, and criminal threat.

Viewed from the realist perspective, a threat to international security becomes obvious when the balance of power is disturbed, i.e. when an individual country becomes too strong, which makes other countries fear for their own security. As a rule, such a development triggers an arms race in an effort to restore the balance of power. The U.S. digital diplomacy programs can therefore pose an international security threat if they disturb the existing balance of power in the international arena and trigger countermeasures. This danger is highlighted by Andrey Krutskikh, Deputy Head of the Department for New Challenges and Threats at the Russian Foreign Ministry. As he puts it, “the main concerns regarding international information security relate to the possibility of information and telecommunication technologies being used for purposes which are incompatible with the goals of maintaining international stability and security.”³²

The fact that digital diplomacy programs are being perceived as a threat in the international arena is demonstrated by the existing trend toward fragmentation of the global information sphere, with individual national and regional segments becoming separate from the global whole. Participants at the informal Shanghai Cooperation Organization (SCO) summit in August 2011 discussed the possibility of setting up information borders to shield the member states from the negative consequences of digital diplomacy.

It is quite telling that large IT companies such as Yahoo!, Google, and others often accept such rules of the game by cooperating with authoritarian governments, passing on confidential information about their users, and blocking some types of search queries. After a brief conflict between Google and the Chinese government in 2010, which was triggered by Chinese hacker attacks against the company’s corporate networks and theft of its users’ personal data, the IT giant resumed operations in the Chinese market.³³ In such a situation there is a clear danger of fragmentation of the Internet, with the World Wide Web disintegrating into isolated segments. Such fragmentation could be achieved through the formation of closed-off intra-national islands within the global Internet, or through launching parallel Internet projects by setting up alternative domain name systems (DNS).³⁴

Another consequence of the power balance being disturbed is an arms race in the information sphere. Back in 2001 Beijing said that given the significant U.S. lead in science and technology, achieving parity with the United States was not feasible, so China would have to rely on information instruments instead. A growing number of countries are pursuing programs to develop such information instruments and to wage information wars. According to the U.S. Government Accountability Office, some 120 countries were pursuing information weapons programs in 2005.³⁵ Lacking the ability to maintain the balance of power internationally, these countries consider such programs to be an appropriate course of action. In addition, several countries are developing concepts for waging information wars, and even attempting to put those concepts into practice. Any further movement in that direction may undermine the existing system of international security and arms control. Martin Libicki, a widely recognized specialist on information war theory, has demonstrated very convincingly in one of his studies that the traditional containment and deterrence methods are not very effective in information space. Information weapons are cheap and easily available to terrorists and criminals, and the source of threats is very difficult to identify with any accuracy.³⁶

Meanwhile, the spread of IT is giving rise to new threats to the leading countries by augmenting the asymmetric component of modern conflict. As a result, technologically advanced nations become vulnerable. Some researchers believe that the U.S. military might and programs to develop information weapons have actually increased the potential for global conflict—for example, by making America’s adversaries feel that they need to acquire nuclear weapons—and have thereby undermined the very international security they were designed to strengthen.³⁷ In addition, IT is obviously having a dual effect on international security. On the one hand, it facilitates democratization (which is the official goal, according to the United States) and thereby reduces the potential for conflict. But on the other, IT is viewed as a convenient instrument for creating asymmetric threats and bolstering political influence, which serves to provoke new armed clashes.



Manuel Castells, a prominent U.S. political and social scientist, offers a somewhat different view of the problem. He believes that the emergence of digital diplomacy should be seen not as an international security threat but rather as a source of new opportunities for addressing and resolving global problems which are too large and complex for any individual state to cope with on its own. Such a mismatch between the scale of the problems and the national capacity for resolving them creates demand for global governance. Global information networks and the social media are opening up opportunities to form a global civil society and facilitate global discourse. In such a context, public diplomacy is viewed not as national diplomacy by governments, but as people's diplomacy, which lays the foundations for national public diplomacy and works on a level above international relations because it is based on shared approaches.³⁸

Discussion of foreign policy and global problems not just by diplomats but by ordinary Internet or mobile phone users can help to strengthen international security by forming a climate of trust in international relations. In such a context, digital diplomacy programs help to establish a universal and globally shared information space, a global civil society, and a new system of global governance which aims to address the crises and problems that affect every country.

It is important to understand, however, that the differences which exist in international relations also exist in the information sphere. According to Castells, the world is heading for a new round of a struggle for power in the global information space. This suggestion is borne out by numerous examples such as systemic censorship of emails in China; the adoption of new EU laws on IT regulation; the acquisition by various actors of social networks in order to track their users' activities and habits; initiatives to introduce network traffic differentiation; and many other processes.

Information has become a key soft power instrument in the international arena. Soft power is based on methods of influence and impact that require communication. The author of the soft power concept, Joseph Nye, defines it in the following way: "Soft power is the ability to get what you want by attracting and co-opting rather than coercion or payment."³⁹ Nye makes a distinction between soft power—which is based on the attraction of the country's culture, ideals, and programs—and hard power, which depends on the country's military or economic might. In his book "The Future of Power" he concludes that in an era of globalized information, the very concept of power in international politics is transformed. Power is now based on information rather than military resources; in an information age, it may be the state (or non-states) with the most favorable presentation that wins.⁴⁰ And that is exactly the goal of the U.S. digital diplomacy programs.

It is no wonder, then, that the growing ability of the United States to project global information influence through various information instruments and digital diplomacy is making countries which are less advanced in that regard feel vulnerable. It is making them want to isolate themselves from the global information space, and to create their own information countermeasures, including programs for waging information wars. The situation is compounded by the fact that some nations view the U.S. digital diplomacy programs as an attempt at meddling in their internal affairs and a threat to their national sovereignty. Such worries are illustrated by regular attempts to block access to Facebook, YouTube, Blogspot, and similar services. At one time or another these websites have been blocked in Vietnam, Iran, Saudi Arabia, Egypt, Pakistan, Burma, North Korea, and several other countries.⁴¹

In this context it is not really important what poses the greater threat to international security: U.S. policies aimed at bolstering American supremacy in the information sphere, or the reaction to such policies by authoritarian countries such as China and Pakistan—a reaction which may result in a fragmentation of the global information space. What is really important is that these U.S. policies and the reaction to them are caused by the very nature of international politics in the information sphere, which inevitably necessitates a struggle for leadership.

The development of spread of IT, including in the area of social networks, offers new instruments for pursuing foreign-policy goals, and for bolstering a country's soft and hard power. Making a distinction between those two kinds of power is not always easy. The United States is trying to strengthen its leadership in the global information space, but even the leaders are becoming vulnerable—and that results in greater international instability. The rise of the World Wide Web is making the traditional mechanisms of international security and stability obsolete. Meanwhile, the new mechanisms, such as multi-level diplomacy and multilateral partnerships, have a long way to go before they become mature.

RUSSIA'S PLACE IN CYBERSPACE

Any analysis of the potential of digital diplomacy for Russia must take into account the current role and the effects of further development of the IT sector on the Russian economy, national security, and political system. Russia is one of the most rapidly and sustainably growing players in the global IT market.⁴² According to the Public Opinion Foundation (FOM), 46 percent of Russians were active Internet users as of late 2011.⁴³ A study conducted by TNS suggests that the most popular social network in the Russian segment of the Internet is VKontakte, which attracts 12 million visitors every day, followed by Odnoklassniki with 7.2 million, and Moy Mir with 5.3 million. Facebook, which has an audience of 1.2 million users per day, scored the highest growth figures.⁴⁴ First websites have appeared in the Cyrillic. рФ domain. The IT sector as a whole generates about 2 percent of Russian GDP.⁴⁵ The Russian Ministry of Communications is working on a list of strategic companies in the Russian Internet industry.⁴⁶ One example illustrating the Russian government's growing attention to the innovative potential of the Internet is that such global IT giants as Google, Cisco, Nokia and Siemens have received invitations to take part in the work of the Russian Skolkovo Fund.

Meanwhile, the importance of IT for Russian national interests is borne out by the continued growth of Internet penetration figures, the economic impact of the World Wide Web, and progress achieved in the area of electronic government. In accordance with the federal program "Electronic Russia" (2002–2010), the development of IT is seen as an instrument for boosting the competitiveness of the Russian economy, facilitating its integration into the global economy, and increasing the effectiveness of national and local government.⁴⁷ Another illustration of the recognition of the innovative potential of the Internet is that the board of the Skolkovo Fund, which oversees the development of the Skolkovo high-tech cluster, includes the chiefs of some of the world's largest IT companies, such as Cisco and Nokia.

Russian government agencies are also increasing their presence on the Internet. The site of the Russian President was launched in 2002, followed by the presidential video blog in 2008, and the presidential Twitter account in 2010. All the federal ministries and agencies now have official websites. In particular, the Russian Foreign Ministry enables Internet users to keep track of the latest foreign policy developments via social networks, including Facebook and Twitter.

At the same time, the Russian government is increasingly focusing on the national security implications of the development of the Internet both in Russia itself and globally. The National Security Strategy until 2020 regards information security as a key component of national security.⁴⁸ It is mindful of the fact that the Internet can be used as a conduit of extremism and terrorism, and an instrument for spreading alien ideology and foreign-policy propaganda. Julien Nocetti, a French researcher, offers an interesting analysis of the Russian government's policy on Internet regulation. He concludes that the government is trying to achieve a fragmentation of the global World Wide Web in order to create a separate Russian segment of it. The main goal of such a policy, the researcher believes, is "to achieve technological independence from global—primarily American—IT players."⁴⁹

Since the early 1990s the Russian government has proposed several initiatives in the area of international information security. One of these initiatives was co-sponsored by Russia and the Shanghai Cooperation Organization in 2011. The Russian delegation at the UN General Assembly proposed a Concept of the Convention on International Information Security, and a draft Code of Conduct in the area of international information security. For now, these proposals have yet to become pieces of international legislation—but they reflect the overall strategy on international information security being pursued by Russia and its allies, and they can yet win broad international support.

Although the Russian government is quite energetic as far as information security initiatives are concerned, it must be recognized that Russia is not making full use of the Internet as a foreign policy and diplomacy instrument, and as a means of bolstering the country's soft power and augmenting its global image. The Internet is one of the drivers of the various globalization processes, and it opens up new opportunities for the Russian government and society. The World Wide Web can serve the task of building up Russia's soft power, forming a positive image of the country in the international arena, and popularizing its rich cultural heritage.

It is important to remember that states are not the only players in the global information arena. There are also the translational media corporations, civil society organizations, communities of



social networks (such as the anti-globalist movement on the Internet), and even individual people. Similarly, an important role in Russia's digital diplomacy should be played not only by government agencies, but also by the commercial sector and civil society organizations. In these circumstances, new multi-level models of international cooperation and diplomacy are beginning to emerge in the framework of the global information sphere. In addition to states, these models include all the aforementioned new actors. Such models are gradually gaining momentum in Russia as well. One example is the Russian Internet Governance Forum, which was launched in 2010. It serves as a platform which brings together representatives of the government, independent experts, and key players in the Russian segment of the Internet and the global information environment.

One of the potentially most rewarding areas of Russian digital diplomacy is to involve Russian high-tech companies in public diplomacy projects. The first steps in this direction have already been made. The trend-setters include Yandex, which is the most popular search engine in the Russian segment of the Internet, and the VKontakte social network, which is popular not only in Russia but also in many foreign countries, including the CIS states, Israel, Germany, and the United States. In recent years Russian IT companies have been rapidly integrating into the global information and innovation community. Examples include the creation of the DST Global fund, which has a global portfolio of IT assets, with stakes in Facebook, Twitter, and Zynga; the acquisition of LiveJournal by SUP Media; and the opening of a Yandex office in Silicon Valley.

An important contribution to the formation of a positive international image of Russian policies and Russian diplomacy is being made by Channel One and RT (the former Russia Today) TV channels, which are both available via live streaming on the Internet. Some Russian government officials and diplomats have launched Russian- and English-language blogs. Government agencies have started to publish freely available reports about their work on their websites. Nevertheless, the IT companies working in the Russian segment of the Internet could be more productively engaged in Russia's digital diplomacy efforts in order to popularize Russian language and culture, and to inform the global audience about Russia's stance on various international issues.

The products and services offered by Russian Internet companies are very popular with Russian-language audiences regardless of where they live. It would make a lot of sense for these companies to promote various initiatives aimed at engaging the Russian diasporas abroad, especially Russian scientists and professionals living and working in other countries. One possible way to facilitate such engagement is to set up a specialized information portal offering up-to-date information on opportunities for cooperation between Russian scientists living abroad and research institutions in Russia itself. The portal would create direct channels of communication and expedite the resolution of various organizational issues standing in the way of such cooperation.

Another promising area for Russian digital diplomacy is to use the potential of crowdsourcing on the Internet. The Help Map project, which was launched for online coordination of relief efforts after the forest fires in the summer of 2010,⁵⁰ has demonstrated that the Internet can be an important instrument of so-called smart crowdsourcing and civil society initiatives, including transnational ones. The Help Map, the Fires Map, and other crowdsourcing projects based on interactive Internet platforms can target not only Russian users but also the global audience. They can enable people to resolve pressing social problems, facilitate civil society initiatives, and make cooperation between the government and the general public more effective. They can also help to form a positive image of Russia abroad. Projects modeled on the Help Map can use social network platforms such as VKontakte, Facebook, and Twitter.


Other practical uses of crowdsourcing for the purposes of digital diplomacy include:

- creating interactive maps of threats and potential dangers, to be discussed at the highest level;
- forming interactive political-diplomatic communities;
- launching platforms to facilitate the exchange of open information about pressing problems, and to establish channels for alerting members of the public during crises.

Using the potential of such platforms to address various problems as part of the Russian diplomatic agenda would enable Russia substantially to increase the effectiveness and reach of its diplomacy in a very cost-effective way.

Russia's effective and innovative growth requires new foreign-policy projects in the digital domain, aimed at bolstering the country's soft power and facilitating the development of science, technology, and education. As the government implements such projects, it must take into account not only the threats posed by the electronic information environment, but also the opportunities. There are effective and proven digital diplomacy instruments, which must not remain the sole preserve of the United States. It is also important to remember that information technologies can evolve and undergo various transformations—but they remain one of the key high-tech products of today's society, and they are making the global world order increasingly network-centric. And that is exactly why government agencies—including those whose remit includes foreign policy—must not procrastinate with putting these technologies to good use.

There is a commonly held view that the latest achievements in the area of IT, including social networks, will never go out of use or disappear as technology continues to evolve. If we accept that view, we can either worry about the possibility of losing control of their content and evolution, or we can recognize that rigid and total control in this area is impossible in any event, and focus instead on gently guiding these processes in a direction which suits our own interests.⁵¹ These conclusions are quite relevant for Russian foreign policy on the Internet. It is important to try to find the right balance between security and a proactive foreign policy in the information space aimed at bolstering Russia's soft power and attraction. The private sector and civil society need to be engaged in efforts to achieve Russia's foreign-policy goals, with the government playing a leading and coordinating role. The provision of information security, on a national as well as international level, remains the responsibility and prerogative of the state.

With such an approach to Russian policy goals in the information space, digital diplomacy could become a valuable instrument for furthering Russia's interests in the international arena. But that will require sufficient investment of intellectual, technological, and organizational resources. Russia has such resources at its disposal—but it is quickly running out of time. That is why stepping up the government's efforts in this area should be seen as an important priority for the immediate future. 

For more analytics on information security, please, visit the section "International Information Security and Global Internet Governance" of the PIR Center website:
net.eng.pircenter.org



NOTES

¹ See: N. Tsvetkova, "Web 2.0 Programs in U.S. Public Diplomacy," *The United States and Canada: Economy, Politics and Culture* No. 3 (2011), pp. 109–122.

² S. Babst, "NATO's New Public Diplomacy: The Art of Engaging and Influencing," *Atlantic-Community*, February 20, 2009, <http://www.atlantic-community.org/index/articles/view/NATO's_New_Public_Diplomacy%3A_The_Art_of_Engaging_and_Influencing>, last accessed January 31, 2013.

³ U.S. Department of State, *IT Strategic Plan: Fiscal Years 2011–2013 Digital Diplomacy*, September 1, 2010, <<http://www.state.gov/m/irm/rls/148572.htm>>, last accessed January 31, 2013.

⁴ Tsvetkova, op. cit., p. 110.

⁵ *World Internet Usage and Population Statistics, World Internet Usage Stats, December 31, 2011*, <<http://www.internetworldstats.com>>, last accessed January 31, 2013.

⁶ A. Slaughter, "America's Edge," *Foreign Affairs* No. 1 (January/February 2009), <<http://www.foreignaffairs.com/articles/63722/anne-marie-slaughter/americas-edge>>, last accessed January 31, 2013.

⁷ Tsvetkova, op. cit, p. 112.

⁸ U.S. Department of State, *21st century statecraft*, <<http://www.state.gov/statecraft/overview/index.htm>>, last accessed January 31, 2013.

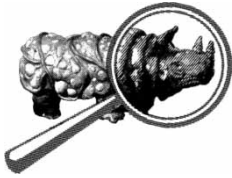
⁹ Tsvetkova, op. cit, pp. 114–116.

¹⁰ *Public Diplomacy: Strengthening U.S. Engagement with the World. A Strategic Approach for the 21st Century*, 2010, <<http://www.carlisle.army.mil/DIME/documents/Public%20Diplomacy%20US%20World%20Engagement.pdf>>, last accessed January 31, 2013.

- ¹¹ L. Khatib et al., *Public Diplomacy 2.0: An Exploratory Case Study of the US Digital Outreach Team*, Oxford Internet Institute, CDDRL working papers No. 120, January 2011, <http://uscpublicdiplomacy.org/media/Exploratory_Case_Study_US_Digital_Outreach_Team.pdf>, last accessed January 31, 2013.
- ¹² Movements.org website, <<http://www.movements.org>>, last accessed January 31, 2013.
- ¹³ Khatib et al., *Public Diplomacy 2.0*, op. cit.
- ¹⁴ White House Official Website, *International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World*, May 2011, <http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf>, last accessed January 31, 2013.
- ¹⁵ U.S. Department of State, *IT Strategic Plan: Fiscal Years 2011–2013 Digital Diplomacy*, September 1, 2010, <<http://www.state.gov/m/irm/rls/148572.htm>>, last accessed January 31, 2013.
- ¹⁶ E. Chernenko, “The State Department’s Internet Protocol Service,” *Kommersant* No. 172 (4713), September 15, 2011, <<http://www.kommersant.ru/doc/1773567/print>>, last accessed January 31, 2013.
- ¹⁷ U.S. Department of Defense, *Department of Defense Strategy for Operating in Cyber Space*, July 2011, <<http://www.defense.gov/news/d20110714cyber.pdf>>, last accessed January 31, 2013.
- ¹⁸ For more details about U.S. approaches to military-political aspects of security in cyberspace, see: Oleg Demidov, “Social Networks in International and National Security,” *Security Index* No. 1 (98) (Winter 2012), pp. 23–6.
- ¹⁹ The White House, *National Security Strategy*, May 2010, <http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf>, last accessed January 31, 2013.
- ²⁰ E. Rogovsky, “The United States: Information Society. Economy and Politics,” *International Affairs* (2008), p. 354.
- ²¹ For more details about the influence of social networks on the social and political processes in the context of the Arab Spring, as well as on national and international security, see: Oleg Demidov, “Social Networks in International and National Security,” *Security Index*, No. 1 (98) (Winter 2012), pp. 23–36.
- ²² A. Chernobay, “The Role of Social Networks in Mobilization of Protest in the Middle East and North Africa in January–March 2011,” *Ideological Aspects of Military Security* No. 1 (2011), <<http://mod.mil.by/iavb/2011n1/9.pdf>>, last accessed January 31, 2013.
- ²³ A. Ross and B. Scott, *Social Media: Cause, Effect and Response*, NATO Review, <http://www.nato.int/docu/review/2011/Social_Medias/21st-century-statecraft/RU/index.htm>, last accessed January 31, 2013.
- ²⁴ See: J. Nye, *The Future of Power* (New York: Public Affairs, 2011), 300 pp.
- ²⁵ S. Aday et al., “Blogs and Bullets: New Media in Contentious Politics,” United States Institute of Peace, No. 65 (August 2010), <<http://www.newmediacenter.ru/wp-content/uploads/2011/10/adayetal2010.pdf>>, last accessed January 31, 2013.
- ²⁶ “Civil Movements: The Impact of Facebook and Twitter,” *Arab Social Media Report* 1 (May 2011), <<http://www.dsg.ae/portals/0/ASMR2.pdf>>, last accessed January 31, 2013.
- ²⁷ E. Morozov, “The Digital Dictatorship,” *Wall Street Journal*, February 20, 2010, <<http://online.wsj.com/article/SB10001424052748703983004575073911147404540.html>>, last accessed January 31, 2013.
- ²⁸ Khatib et al., *Public Diplomacy 2.0*.
- ²⁹ Quote from: Khatib et al., *Public Diplomacy 2.0*.
- ³⁰ V. Kulagin, “Global or World Security,” *Mezhdunarodnye protsessy* No. 14 (2006), <<http://www.intertrends.ru/fourteen/004.htm>>, last accessed January 31, 2013.
- ³¹ See: Oleg Demidov, “International Regulation of Information Security and Russia’s National Interests,” *Security Index* No. 4 (101) (Fall 2012), pp. 15–32.
- ³² A. Krutskikh, “On the Political and Legal Framework of Global Information Security,” *Mezhdunarodnye protsessy* No. 1 (5) (2007), <<http://www.intertrends.ru/thirteen/003.htm>>, last accessed January 31, 2013.
- ³³ See: “Google returns to China,” *Vedomosti*, January 13, 2012, <http://www.vedomosti.ru/tech/news/1473990/konec_bojkotu>, last accessed January 31, 2013.
- ³⁴ See: “The Future of the Internet: A Virtual Counter-revolution,” *The Economist*, September 2, 2010, <<http://www.economist.com/node/16941635>>, last accessed January 31, 2013.
- ³⁵ A. Krutskikh and I. Safronova, “International Cooperation on Information Security,” Information and Communication Technologies in Education portal, <<http://www.ict.edu.ru/ft/002472/intcoop.pdf>>, last accessed January 31, 2013.

- ³⁶ See: M. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND Corporation, 2009), <<http://www.rand.org/pubs/monographs/MG877>>, last accessed January 31, 2013.
- ³⁷ R. Bolgov, *IT in Modern Armed Conflicts and Military Strategies (Political Aspects)*, author's summary of a PhD thesis (St Petersburg: SPbGU, 2010), pp. 12–13.
- ³⁸ M. Castells, "The New Public Sphere: Global Civil Society, Communication Networks, and Global Governance," *Annals of the American Academy of Political and Social Science* No. 616 (2008), <http://prtheories.pbworks.com/w/file/etch/45138545/Castells_2008_The_New_Public_Sphere.pdf>, last accessed January 31, 2013.
- ³⁹ J. Nye, *Soft Power: The Means to Success in World Politics* (New York: Public Affairs, 2004), 191 pp.
- ⁴⁰ Nye, *The Future of Power*, op. cit.
- ⁴¹ Freedom House, "Freedom on the Net: A Global Assessment of Internet and Digital Media," April 1, 2009, <<http://www.state.gov/documents/organization/135959.pdf>>, last accessed January 31, 2013.
- ⁴² Federal Program, "Electronic Russia (2002–2010)," Internet i Pravo law firm, March 2, 2010, <<http://www.internet-law.ru/intlaw/laws/e-rus.htm>>, last accessed January 31, 2013.
- ⁴³ Public Opinion Foundation, "Internet in Russia: Methods and Key Results of the Study," *Analytical Bulletin* No. 33 (Spring 2011), <<http://bd.fom.ru/pdf/Internet%20v%20Rossii%20vol%2033%20vesna%202011%20short.pdf>>, last accessed January 31, 2013.
- ⁴⁴ A. Gavrilyuk, "Number of Russian Internet users up 14 per cent from last year," *RBC Daily*, February 10, 2011, <<http://www.rbcdaily.ru/2011/02/10/media/562949979689739>>, last accessed January 31, 2013.
- ⁴⁵ "Russia Online: The Impact of the Internet on the Russian Economy," a report by Boston Consulting Group, May 1, 2011, <<http://img.rg.ru/pril/article/48/57/59/000111333.pdf>>, last accessed January 31, 2013.
- ⁴⁶ E. Koshkina, "Russian Government to Keep Tabs on Foreigners' Investment into the Internet," *Kompyulenta*, April 9, 2009, <<http://net.compulenta.ru/417783>>, last accessed January 31, 2013.
- ⁴⁷ Federal Program, "Electronic Russia (2002–2010)," approved on January 28, 2002. Russian Cabinet Resolution No 65, <<http://www.internet-law.ru/intlaw/laws/e-rus.htm>>, last accessed January 31, 2013.
- ⁴⁸ "Russian National Security Strategy until 2020," Russian Foreign Ministry website, <<http://www.mid.ru/ns-osndoc.nsf/0e9272befa34209743256c630042d1aa/8abb3c17eb3d2626c32575b500320ae4?OpenDocument>>, last accessed January 31, 2013.
- ⁴⁹ J. Nocetti, "Digital Kremlin: Power and the Internet in Russia," Russia/NIS Center, April 2011, <http://www.pircenter.org/kosdata/page_doc/p2734_1.pdf>, last accessed January 31, 2013.
- ⁵⁰ Help Map, "Helping the Victims of Fires," Internet portal, <<http://www.russian-fires.ru>>, last accessed January 31, 2013.
- ⁵¹ See, for example: J. Lichtenstein, "Digital Diplomacy," *New York Times*, July 16, 2010, <<http://www.nytimes.com/2010/07/18/magazine/18web2-0-t.html?pagewanted=all>>, last accessed January 31, 2013.





Arnaud Leclercq

RESILIENCE OF RUSSIA

The last 20 years saw successively the collapse of the Soviet Union and establishment of the Russian State, which one could think was at the time under threat of being drawn into terrible political, economic, and social crises caused by the events of 1991. Absolutely imperceptible until the turn of 2000, a revival created a new situation when Russia, consolidated inside its borders, managed to regain its weight and influence in the international arena.

The renaissance of Russia as a power fits into the general context of the emergence of a rather unexpectedly multipolar world, taking into account the prospects which the end of the Cold War opened to the Benevolent Empire of George Bush. Professor of Harvard University Francis Fukuyama prophesied the “end of History,” the summary of which was supposed to be a universal triumph of Western-type democracy and generic establishment of a market economy. Putting aside all comments on the internal situation in Russia with its corruption and other aspects related to human rights, it should nevertheless be accepted that the achieved international revival became possible, to a great extent, due to the authority and abilities of Vladimir Putin. He knew to mobilize around himself the new elite leaders, determined to make the modernization of the country a success without sacrificing at the same time their ambitions to power. Having come through Peter the Great’s Westernization and reforms by Alexander II or Soviet revolutionary projects, on the eve of the twenty-first century Russia, which has faced relative failures throughout its history, has probably entered a context that can appear favorable provided that the country knows how to play its numerous trump cards, a historic sequence that can put it back into the first rank in the generally balanced world that is gaining shape, even if in a very uncertain manner.

After the Soviet period and its universal revolutionary projects born of the big October 1917 breakthrough, the final failure of communist messianism and the collapse of the empire inherited by the Bolshevik regime from tsarist times constrained Russia from defining its renewed identity. It relies on the great patriotism based on a commitment to the “Russian soil,” a strong historic consciousness and a rich cultural heritage together with a revived orthodox tradition, not to mention the memories of the Great Patriotic War, the victorious outcome of which is still attributed to Stalin despite the crimes of the regime he nurtured for 30 years. Russia’s renewed identity does not rule out its proximity to Europe towards which, as was the case in the time of Peter the Great, Russia is still heading as its priority direction although the European Union, attached to the Atlantic Bloc, has on numerous occasions given it reasons for disappointment.

GRAVITY CENTER SHOULD SHIFT TO ASIA

Leaving Europe aside for a while, it is important to note that the gravity center of Russia is shifting today to Asia. Historically, the West virtually always posed threats to Russia’s interests and security (Lithuania, Poland, Sweden, Germany, France, England, etc.) while the East offered rather easy gains, and enormous Asian territories were preserved regardless of the downfall of the tsarist empire and disappearance of the Soviet Union. In modern times, the proposal of Mikhail Gorbachev to create a Common Home was turned down by European chancellors. The support



A
N
A
L
Y
S
I
S

provided to the United States by Vladimir Putin after the September 11 events was reimbursed by increased American influence in the “near abroad” either through the so-called spontaneous color revolutions or deployment of missile defense systems in Poland and the Czech Republic to protect them from theoretical aggression coming from Iran. On December 10, 2011, in the Swiss daily *Le Temps*, the head of Russia’s Permanent Mission to NATO, Dmitry Rogozin, stated that “the Americans took Russians for fools in this situation.” Apart from the reinforced partnership with Germany and even France when it was still headed by Sarkozy, Russia was globally disappointed by the West. Moreover, the crisis that was generated by American loans plunged the European economies into a recession that risked resulting in a depression and collapse of the Eurozone. Why should Russia now have any interest in continuing to look towards Europe?

In parallel, the Asia-Pacific zone does not create any problems for Russia: there is no criticism of the human rights situation or missile defense or color revolutions but instead strengthened diplomatic, economic and military cooperation. Provided that the challenges of infrastructure modernization, exploration, and exploitation are addressed—regardless of the remaining difficulties—the volume of energy resources can in the mid-term prospectively become the best trump card, because Russia will find itself in the situation where it will supply gas and oil to Europe and the Far East—two well-populated and dynamic areas where Russia’s resources are badly needed from now on. These resources must give Russia the means to develop and modernize its communication lines, railways, roads, and air routes, all of which will be indispensable to manage a territory of exceptional dimensions. During the Asia-Pacific Economic Cooperation (APEC) summit in Vladivostok in September 2012, to respond to the growing energy demands of Asia, Russia announced a threefold increase in its oil supplies during the next decade. In 2020, consumption by Japan, South Korea, and China will represent 50 percent of world energy consumption. Moreover, after the catastrophe at Fukushima NPP, Japan decided to close almost totally its nuclear park and, therefore, has to turn to Russia as a supplier while European demand could face stagnation. But it is most important to note that the price of the gas sold to Asia is, at \$600 to \$700 per thousand cubic meters, practically equivalent to oil prices, and is half the price proposed to Western Europe.

RELATIVE STABILITY

Humiliated and incapable of influencing the events in the 1990s, Russia has regained strengthened initiative and freedom of action, which are being used effectively by its authorities in the interests of the foreign policy project launched by Vladimir Putin during the Munich Conference in 2007. Russia is benefiting from the implementation of this project by regaining its political stability and, despite certain controversies, the re-election of Vladimir Putin as President is the confirmation thereof. This is a major trump card for the coming years at a time when the West is affected by crisis and the ambitions of China and emerging countries are pushing the balance of forces in the world. This is also an advantage in the face of considerable challenges that Russia needs to overcome to assure its economic modernization.

Conversely, Russia aligns itself favorably with European democracies in terms of uncontrolled immigration and Islamist factions that are giving rise to growing concerns among the population of the relevant countries. Thus, taking into account the 80 percent of Russians who live within the borders of the enormous Federation, the question of minorities no longer matters, and the attempts to achieve autonomy and independence demonstrated in the Caucasus and “Turkish” republics on the Volga River at the beginning of 1990 are of no importance today. This has given rise to decentralization of power and economic growth, which should prove beneficial for the regions in question. During recent years Russia has also made a remarkable return to the “near abroad” from whence allegedly came the American rollback. The crisis that affects the whole of Europe may likely re-direct Belarus and even the Ukraine towards Russia, and such an evolution is even more visible in the former Soviet Central Asia, in particular in Kazakhstan and Kyrgyzstan. A pragmatic alliance with China established through common interests to respond to the initiatives of Washington in Central Asia is beneficial for both parties, even if one day the two partners may turn into rivals in the emerging multipolar world in which the United States and Europe face a relative loss of influence. Such conditions seem to be favorable to Russia’s ambitions today. However, a handicap that gives great concerns is the demographic situation in the country, which has for many years been facing a continuous decline in population.

RUSSIA, EURASIAN POWER

The Eurasian position of the country¹ is, incidentally, a considerable geo-strategic advantage that makes Russia and its provinces the obligatory passageway of the new continental Silk Road which could in the mid-term replace the commercial sea routes controlled by American thalassocracy. In 2001, Russia made considerable investments in its road and railway infrastructure. As for the sea routes, the forecast climate change that is commonly considered as a threat may, in contrast, become beneficial for Russia, the very northern part of which endures climatic conditions that until now have constituted a serious obstacle to development. The prospects that prevail in the Arctic, in particular in the area of oil and gas exploration, as well as disclosure of an inconceivable sea route that now opens up an ocean space to Russia, which has been a prisoner of its continentality for a long time, evidently have positive consequences in store. The mass media now constantly refer to the energy potential of the Arctic² regardless of the enormous difficulties caused by the climate as demonstrated by the dropping of the giant Shtokman project. At the same time, according to a 2008 study by the U.S. Geological Survey, the Arctic Circle contains 13 percent of world oil reserves and 30 percent of natural gas.

For several years already and in spite of the devastating consequences of the drought of 2010, Russia has been enjoying its agriculture potential which was compromised during Soviet times by the burdens and failures of agricultural collectivism. It is possible to imagine that in the mid-term, in a world where the demands for food products will grow due to a rapid growth in population, Russia will again be able to play a role comparable to its role before 1914 when it provided almost half of the world market with grain. This is a very important geopolitical benefit taking into account the needs of sub-continental India, the Middle East and Africa.

Finally, in a very short time Russia managed to withstand a terrible test posed by its transition from the status of superpower, established in the bipolar world of the cold war, to forefront power, an actor born to play such a role in the new emerging international concert. The disappearance of a Soviet people the leaders of the USSR were dreaming of and the return of the Russian nation is the first step in the country's ongoing re-composition. The integration of the Muslims of the Northern Caucasus still remains a problem because of the history of conflicts and the complicated geopolitical situation of the region. However, attempts to gain autonomy and even to become independent of certain minorities, in particular in the Volga region, did not threaten the territorial integrity of the Russian Federation which arose from the remains of the USSR, and today Tatarstan is a dynamic region with new Muslim traditions stripped of any fundamentalism. In general, following the breakdowns observed in the 1990s when Russia seemed to be subject to centrifugal forces rooted in the excessive autonomy acquired by the regions, which appeared to become favorable for the emergence of local powers connected with particular clients, the regained central power allowed the restoration of the Power Vertical and contributed to a strengthening of national unity, which was in a visibly bad state during the Yeltsin era.

HUMAN RESOURCES

A revived Russian consciousness was among the necessary prerequisites of Russia's return to the international arena but there is one matter that still appears to be outstanding. This relates to the demographic development of the country, which could become dangerous for the future if it is not rapidly reversed. Russia, which benefited from an impressive fecundity until the 1960s—to the level of addressing and overcoming the terrible bloodshed of two world wars, revolution, civil war, and Stalin's terror—appears to face today a decrease in population that could be a danger. Moreover the maternity support measures announced by the government have not allowed hopes to be justified although they have brought about practical improvements. The deficiencies observed in healthcare, in particular in the area of individual medical care, are the reason for the reduction in life expectancy in Russia, where the problem of alcohol still remains widespread. The situation may improve with the economic progress that human resources should give to Russia. However, nothing has yet been achieved and it will not be possible to reveal the major potential benefits of the enormous Siberian area without the existence of human resources sufficient to explore it, especially taking into account the enormous demographic discrepancies between the Russian Middle East and the densely populated area of Eastern Asia.

However, the resistance capabilities of Russia's education system also appear to be a benefit inherited from the Soviet era to reveal the deficiencies in a knowledge- and innovation-based



economy when speaking about preserving Russia's place in certain areas such as the space industry, a military and industrial complex, nanotechnologies which are considered indispensable on the way to economic power, and management of the technologies of tomorrow. After the times when certain oligarchs brought up by the former communist system wasted the country's resources for the sake of privatization the State managed to regain control over the resources that give it the capacities to exercise its power. However, it is only with the help of different and supplementary layers – and not the layer of *siloviki* coming from the “services” the Russia-hostile Western media regularly talk about – that today's leaders of the country will be able to restore governmental elites capable of ruling efficiently for a long time and address the scourge which is still represented by corruption. Exactly like Peter the Great and Catherine II, Vladimir Putin and Prime-Minister Dmitry Medvedev could invite some high-level foreign experts to help to manage financial institutions or major public enterprises, in particular in dealing with foreign trade or to improve the perception of Russia among Western decision-makers.


Such an attitude seems to be indispensable if Russia wishes to prevent the outflow of its elites at a time when the world's most dynamic economic poles are trying to attract the best brains and holders of the most sophisticated know-how. The new Russia should also take advantage of the Russian language, as in the former Soviet Empire, to make it a valuable tool of influence in the near abroad where attempts to switch to the Latin alphabet or to increase the role of English as an international language may threaten the cohesion of the continental geopolitical space. Rooted in the long orthodox memory of Russia's historic consciousness, its attachment to the literature heritage of the “Great Russian Century” or memories of sacrifices during successive interventions forms an inalienable element of identity proof at a time when, unlike Europe, which is reduced to amnesia out of fear of admitting its Christian origins and identity, all huge civilizations turn towards their roots to endanger Western universalism.

NEW SPACES

The renaissance of Russia is also seen through the management of spaces in terms of geography, policy, and economy; such was the discovery of the tsarist and Soviet empires and it remains a major advantage. For today's Russia this implies the improvement of its transport such as trains, roads, and planes; a lot is still to be constructed in these areas even if, regardless of the reduction of sea gates following the demise of the USSR, the declared climate change does open up unprecedented ocean spaces through the Arctic Ocean. For the West it is difficult to imagine the range of changes at the beginning of the 1990s when Russia became open. As a result, the whole geographic economy has undergone transformations and most industrial regions inherited from the Soviet Union have revealed weaknesses because of the prioritising of heavy industry, enterprise giantism, or excessive specialization practiced by the administration economy. A considerable adaptation effort should be made, and even if the Center organized around Moscow seems with success to be addressing the challenges of rapid modernization, the evolution will apparently not be that fast in some regions where serious burdens evidently remain. Along with the construction of the new Russian economy, which cannot reduce itself solely to the exploitation of energy and raw materials, the State will become capable of advantageous international influence.

The second decade of the twenty-first century has started in a context which is more likely to be favorable for a Russian power undergoing progressive reconstruction which is capable, notably within the framework of BRICS (Brazil, Russia, India, China, and South Africa)—the new “emerging” powers—to have more impact on international relations while the Western hegemony seems to be clearly under threat. Leaving aside the United States and Europe, direct contracts with these “developing countries” should successfully grow in number. In this context, it is worth noting as an example a contract concluded in March 2012 among central banks of the said countries aimed at developing their trade without resorting to the dollar.

With many advantages in hand, Russia should also take into account the major challenges and uncertainties of the beginning of the twenty-first century. Today, it has to find its place in the newly emerging balance of powers. It has to redefine and reaffirm its specific identity in the world, where the return of vast civilization spaces threatens the claims of the West to universality. It is among the states that can benefit from climate change, even if the latter is considered a danger at the level of the planet. In a world where energy consumption will grow and which will have to feed its rapidly growing population, its resources will allow it to find a good position from which to

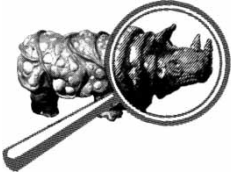
influence with all its weight in all these different areas. With its Euro-Siberian location—and bearing in mind its resources and major geostrategic situation—it can preserve the pure Russian representation of its identity and environment while remaining open to Europe. Destined to regain its place as a major power but probably also in the future having to face the Chinese threat hanging over the Russian Far East or dominance in Central Asia, the future Russia will be also formed by the relations it establishes with Western Europe, which has itself been isolated from the Euro-Atlantic space dominated by the United States. Yes, we can affirm that Russia has never been as strong as it is when it sees itself not simply as a West-oriented European power. 

NOTES

¹ See also: Arnaud Leclercq, “La Russie, puissance d’Eurasie, Histoire géopolitique des origines à Poutine,” *Ellipses*, November 1, 2012.

² See *The Financial Times*, September 5, 2012 or *Swiss Daily*, September 20, 2012.





Eldar Kasayev

QATAR: RUSSIA'S AMBITIOUS COMPETITOR ON THE GAS MARKET

Russia and Qatar seem very different at first glance—but the two countries actually have a lot in common. For example, even though both are trying to diversify their economies, they remain strongly dependent on exports of raw materials. Indeed, oil and gas exports generate a huge part of their budget revenues.

BILATERAL ECONOMIC STAGNATION

The development of trade and investment ties between Russia and Qatar is currently at a very low level. In 2010 bilateral trade stood at a measly \$14.5–14.6 million, of which Russian imports (organic chemicals, plastics, and rubber) accounted for \$11.1–11.2 million. Qatari imports from Russia—precious and non-precious metals (\$2 million), timber (\$0.9 million), machinery and transport, equipment, and instruments (\$0.5 million)—stood at only \$3.4 million (see Table 1). In 2009, Russian–Qatari trade stood at only \$8.7 million. In January–February 2011 it was only half the figure for the same period in the previous year (\$1.7 million and \$3.4 million, respectively).

It is safe to assume that bilateral trade between Russia and Qatar will shrink even further over the coming years because the two countries' political relations have recently soured, putting a damper on economic cooperation. Even in 2010, when the level of political dialogue between Moscow and Doha appeared to have reached new highs,¹ Qatar ranked 139th among Russia's 140 biggest trading partners, narrowly beating Cameroon.²

Looking at Qatar's trade with its key Asian and European partners over the past decade one can assume that Qatar consistently has a large trade surplus with the Asian countries (with the exception of China) thanks mainly to exports of hydrocarbons. Exports to and imports from China were relatively well balanced in 2002–2006. In the following two years Doha had a trade deficit with Beijing, which turned into surplus in 2009–2010 on the back of growing Qatari gas exports to China.³

Qatar had a steady trade deficit with Europe in 2002–2009; predictably, that deficit peaked with the onset of the world economic crisis. But the figure then swung into surplus in 2010, reflecting not so much an economic improvement in Europe as the continent's growing imports of Qatari fuel in an attempt to reduce dependence on Russian energy.

Meanwhile, Russian–Qatari trade has been languishing even despite the existing legal framework for economic cooperation, including the bilateral agreements on economic, trade, and technical cooperation (1990); on avoidance of double taxation (1998); on mutual protection and encouragement of investment (2007, not yet ratified by Russia); on cooperation between the two countries' Chambers of Industry and Trade (2001); and on establishing a Russian–Qatari Business Council (2007).

Aware of the existing imbalances, the two countries have undertaken constructive efforts on the institutional level. They have set up the Russian–Qatari Commission for Energy and Gas, and



Table 1. Russian–Qatari Trade in 2009–2011 (\$ million)

Time period	Trade				Growth		Share of total
	2009	2010	Jan–Feb 2010	Jan–Feb 2011	2010 on 2009	2011 on 2010	2010
Total	8.7	14.6	3.4	1.7	66.8%	– 48.9%	100%
Agricultural products				0.0		100%	
Chemicals, plastics, and rubber	7.2	11.2	3.0	1.4	55.6%	– 52.3%	76.6%
Leather and leather products	0.0				– 100%		
Timber	0.6	0.9	0.3	0.2	56.1%	– 21.9%	6.2%
Textiles and footwear	0.0	0.0			66.4%		0.2%
Precious and non-precious metals and products	0.0	2.0	0.1	0.0	10894.5%	– 99.9%	13.7%
Machinery, equipment, transport, and instruments	0.9	0.5	0.0	0.1	– 48.1%	113.5%	3.4%
Other	0.0	0.0		0.0	– 84.6%	100%	0.0%

Source: Russian Ministry of Industry and Trade.

agreed to establish an intergovernmental commission on trade, economic, science, and technical cooperation.

Meanwhile, Russia has clearly demonstrated that there are real opportunities for bolstering bilateral trade. In 2010 two large delegations from the Urals Federal District visited Qatar. As part of the first visit, Doha hosted the first Russian–Qatari economic forum headlined “Current State, Opportunities and Prospects for Cooperation between Qatar and the Ural Federal District”; the event was held in cooperation with the Qatari Business Association.

During the second visit Russian and Qatari representatives discussed possibilities for Russian food exports to the emirate. As a result of the two visits, several Russian companies—including the Urals Mining and Metallurgy Company, the Pipes and Metals Company, Ural Industries–Ural Polar, and Seligdar—established contacts with partners in Qatar. Ural Industries–Ural Polar and Seligdar later invited Qatari companies to invest in Russian gold mining projects.

According to an annual report by Gazprom, in December 2010 the Russian gas giant opened a representative office in Qatar in order to facilitate long-term economic cooperation with the emirate, and to represent the company’s interests in the Middle East. Gazprom’s plans include cooperation with state-owned oil and gas companies in Qatar and other Gulf states, as well as coordination of the work of Gazprom subsidiaries in the regional energy markets.

In actual fact, however, the Gazprom office in Doha has yet to commence operations because the Russian company has been unable to obtain commercial registration—even though Qatari registration documents are typically issued within a week. Nevertheless, the Russian gas monopolist hopes to establish itself in Qatar and to take part in joint gas and LNG projects after the lifting of the moratorium on increasing production at the North Field, which was imposed by the emirate’s authorities in 2005. Doha has said that the moratorium will expire in 2014—but that may yet change (there was a precedent in 2009, when the moratorium was extended just before it was due to be lifted).

Besides, Gazprom may yet have to make serious adjustments to its plans in view of the typical government and business culture in the Arab countries, which is notorious for long delays and stifling red tape.

In 2010–2011 Russia invited the Gulf emirate to invest in numerous projects in the oil and gas sector, gold mining, construction, and other industries. Had these projects come to fruition,

Qatari investment in the Russian economy could have reached about \$10–\$12 billion. But Doha has not accepted any of these proposals.

Qatari businesses do not seem to have any real interest in working with Russia. The hopes for dynamic economic cooperation between the two countries, which have been voiced following official visits to Russia by senior Qatari officials, do not appear to have any solid foundation. There are several concrete examples to support such pessimism.

First, the Qatari side, based on inaccurate estimates by its experts, has walked away from the proposed acquisition of a 10-percent stake in Russia's VTB bank—even though the state-owned Russian company was prepared to sell that stake at a discount (for \$2.5 billion instead of \$3 billion). As a result, the bank, which had a clear instruction from the government to sell a 10-percent stake before February 15, 2011, was forced to turn to Western investment funds instead. In the end, the shares were sold for \$3.3 billion.

Nevertheless, VTB has since told the Qataris that at some point in the future it might be prepared to offer another stake for sale—but the price would be significantly higher this time around. At first, Qatar seemed to express a great deal of interest in that second proposal—but that interest has gradually fizzled out, and the whole deal has been put on hold.

Second, VTB Capital (the VTB bank's investment division) invited Qatar to participate in the development of two medium-sized gas fields after holding a presentation of the investment project in July 2010. The two sides held talks, but in the end failed to reach an agreement.

Third, in 2010 several Russian companies invited Qatar to invest in several gold mining and property development projects. After waiting for eight months for a clear response from Qatar—which never came—some of those companies were forced to sign deals with other foreign partners, which wasted no time at all and gave a positive answer almost immediately.

Fourth, one of the first investment projects proposed to the Qataris was Yamal-LNG, led by Novatek, a leading independent Russian gas producer. But once again, after seeming to express some interest, the Qataris dithered, and the proposed deal fell through. A similar fate befell several other proposed projects in such areas as water desalination, high-tech industries, and the food industry.

The present author is deeply convinced that the problem stems primarily from the unprofessional and biased attitude of Western specialists working for Qatari companies. Very often these specialists deliberately submit inaccurate information, drag their heels on various projects, and fail to communicate in a timely manner, responding to various Russian queries so late that they might as well not have bothered. American, British, and Australian citizens, as well as representatives of other countries which are antagonistic to Russia, often have a lot of influence on how the Qataris react to Russian investment proposals. They often do their best to prevent Russian businesses from carving out a niche for themselves on the Qatari market because they do not want Western companies to face any Russian competition. As a result, large Russian companies—let alone small and medium businesses—have been all but barred from Qatar.

A case in point is the failed deal to acquire a 10-percent stake in VTB. The Western specialists involved in the talks were drawing salaries from the Qataris—but they were in fact working for their own Western countries. In the end, the Russian state-owned bank sold the stake to U.S. and British investment funds, while Qatar lost \$800 million which it could have made by buying the stake at a discount.

In order to overcome this problem, measures need to be taken in order to outplay these foreign advisers, who not only prevent the two countries from doing mutually profitable business, but also complicate political relations between Russia and Qatar.

Clearly, the glut of Westerners in Qatari companies makes it difficult for Russia to secure a strong presence in the emirate's economy. However, the misguided priorities of many Russian businessmen do not help, either. Instead of effectively defending the economic interests of their country in line with international standards, and instead of doing their best to promote Russian projects in Qatar with long-term goals in mind, Russian business leaders merely try to secure a quick profit during their fleeting appearances in the emirate. Their priorities do not include systemic and large-scale efforts to secure a solid reputation for their companies, or to study the supply and demand situation in the Qatari market.



Neither should we discount the Qatari business mentality, which also plays an important role. The Qataris do not aim to earn a quick buck in circumvention of their own country's laws; on the contrary, they want to see that their foreign partner has a serious intention to cooperate on a long-term basis. That is why those of the Russian companies that have not abandoned hopes for cooperation with Qatar should follow in Gazprom's footsteps and open offices in Doha.

By the end of 2010 the size of the Qatari state-run reserve fund had reached about \$110 billion,⁴ enabling the emirate to make serious investments in large foreign projects, including the purchase of stakes in foreign companies.⁵

It is therefore clear that Doha's reluctance to invest in Russia cannot be put down to the lack of funds. On the one hand, Qatar is waiting for the consent of the United States and Britain, which essentially steer many of the country's foreign economic activities. On the other hand, Russia itself is not demonstrating genuine interest in effective financial cooperation because it does not want to play by the business rules which the Qataris expect from their partners—and which the Western companies are happy to play along with.

GAS EXPORTING COUNTRIES FORUM: FAILED EXPECTATIONS

It is possible that closer and more effective cooperation between Russia and Qatar can be facilitated by the Gas Exporting Countries Forum (GECF).⁶ There is a clear paucity of research and analysis regarding the organization's activities and prospects. Worse, those few publications that are available tend to contain inaccurate or unconfirmed information. For example, journalists and experts often describe the GECF as a "gas OPEC." Such a description completely misrepresents the nature and the stated goals of the organization.

To begin with, let us look at the GECF background. The forum was set up as an informal club in 2001, and later became an official international organization. The decision to that effect was taken on December 23, 2008 at the 7th Ministerial Meeting of GECF members in Moscow. That is when energy ministers of the participating countries approved the organization's statute and signed the relevant intergovernmental agreement. The ministers also chose Doha to host the GECF headquarters.

In accordance with the Statute, the GECF has three governing bodies: the Ministerial Meeting (usually held once a year); the Executive Board; and the Secretariat. The Ministerial Meeting is the supreme governing body; the Executive Board runs GECF affairs between the meetings. The Secretariat, led by the Secretary-General, is in charge of technical and organizational issues. The financing comes from the contributions of the participating states.

In December 2009, during another GECF ministerial meeting, a Russian candidate was unanimously elected as the organization's Secretary-General. The decision was widely expected. In 2008 GECF members turned down the Russian proposal to set up the organization's HQ in St Petersburg, choosing Doha instead. Understandably, the emirate decided not to oppose the election of a Russian representative as secretary-general.

It must be said that diametrically opposed views were aired when the GECF was being set up. But it would be completely wrong to describe the organization as a "gas OPEC" because its statute does not contain any mechanisms for regulating gas prices. On the contrary, the GECF is not allowed to impose quotas on gas production. Its main objective, as stated in the statute, is to support the sovereign rights of member countries over their natural gas resources and their abilities to independently plan and manage the sustainable, efficient, and environmentally conscious development, use, and conservation of natural gas resources for the benefit of their peoples, as well as to facilitate the exchange of experience, views, information, and coordination in key areas of the gas industry.

Some of the GECF members support, to a greater or lesser degree, the idea of turning the forum from a platform for discussion into an effective international organization capable of influencing the price formation mechanism in natural gas exports. In particular, this proposal has the support of Iran, Russia, Algeria, and Venezuela. Between them, the four countries control more than 50 percent of the world's natural gas reserves. These countries' wish to regulate the cost of this energy source for consumers is entirely natural and legitimate—but such regulation is a far more complex task than it might appear at first glance.

The first thing to take into account is that, unlike oil, gas is not traded on a single global market. Instead, there are a large number of smaller regional markets, which are all different in terms of supply and demand. That is why the suppliers are working hard to diversify the geography of their exports, and compete fiercely with each other in the process. For example, Qatar has plans to increase gas exports to Europe, thereby creating certain difficulties for Gazprom, as well as for Algeria's Sonatrach. Meanwhile, Russia has ambitious plans with regard to the Asian markets—which Qatar views as the main destination for its own gas exports.

Second, there are complications in the area of domestic and foreign policy. The Arab uprisings in 2011 have resulted in a change of regime in several Middle Eastern countries, and shifted the balance of power in these countries' energy politics. Egypt and Libya have fully felt the consequences of those changes.

Third, it is necessary to take into account the different gas policies of the exporting states. Most of them—including Russia—export gas mainly via pipelines under long-term contracts. As a result, they are interested in maintaining the stability of annual supplies, for which they charge a fixed price that does not fluctuate depending on the market situation. In the long-term contracts used for gas exports via pipelines, the gas price is aligned with the price of oil and is calculated using a pre-determined formula.

In contrast, Qatar is interested in short-term contracts at spot prices, which depend on the current market situation and are not linked to any long-term arrangements. Russia, on the other hand, argues that the GECF should develop a mechanism for market-based gas price formation which could be used by the suppliers for new long-term contracts.

According to Doha, the best way of achieving stability in the global energy markets is to link the price of natural gas to the oil prices. If the gas exporters can agree on using such a price formation mechanism, the gas markets will become accessible to everyone because that mechanism would obviate the need to choose the export destinations depending on the price offered by the individual importers.

Nevertheless, Qatar is opposed to the idea of creating a gas cartel. Exporters and importers alike are actively debating the idea of setting up a proper OPEC-like outfit for natural gas. Countries such as the United States, Canada, Australia, and many EU members are vehemently opposed to this. Qatar is forced to take their stance into consideration; it does not want to be accused of entering into a cartel agreement and see the issue being brought to international arbitration.

This is why Qatar avoids any discussions on developing a real price-formation mechanism for gas supplies, arguing that the exporters should just sell their gas to consumers at the highest price they can charge—which is exactly what the emirate is doing now.⁷

All of these geopolitical, economic, geographic, and some other factors are preventing the suppliers from agreeing a clear common stance on exports. It would therefore be premature to talk about GECF evolving into an organization that can effectively dictate prices to consumers by coordinating the positions of the main gas exporters. There is also a strong impression that even though the GECF has held its first Gas Summit, the organization has yet to fully mature.

In July 2010 the GECF Executive Board held an extraordinary meeting, during which the Secretariat presented a concept of the Global Gas Initiative. The proposal included the establishment of the International Gas Institute; the launch of a PR campaign to promote natural gas in new markets; developing a gas supply and demand modeling mechanism; and setting up a special fund to finance all of these activities. The participants decided that it would make sense to use these proposals for drawing up a long-term GECF strategy.

In September–October 2010 the GECF Secretary-General paid several working visits to Malaysia, Brunei, Libya, Egypt, and Equatorial Guinea. He also held consultations with UN Secretary-General Ban Ki-moon to discuss the prospects for cooperation between the GECF and special UN bodies.

On December 2, 2010 the 11th GECF Ministerial Meeting approved the Secretariat's proposals on the organization's strategy and plans for 2011–2015. It also instructed the Secretariat to set up a research division, and agreed to initiate the development of a gas market simulator model. Finally, the meeting approved the decision to hold the First GECF Gas Summit, to be attended by heads of state or government, in Doha on November 15, 2011.



In other words, the Secretariat is making organizational efforts to turn the GECF into an effective specialist organization which could further the interests of its participants. But the present author believes that at this point the organization is merely proclaiming the need to develop a global gas market model and a long-term development strategy for the GECF itself. In practice, however, the GECF has not begun to fill that initiative with any real substance; in fact, it has not even completed preparations for such practical work.

The GECF has so far failed to achieve any of its key objectives, such as: ensuring the security of supply and demand on the gas market; facilitating new investment in the gas industry; or developing a coordinated and consolidated position of the GECF member states in the global energy dialogue.

Let us recall that during the talks to formalize the GECF and draw up its founding documents Russia proceeded from the notion that creating a specialist organization of gas exporters, modeled on the existing OPEC oil cartel, would include some kind of a market-sharing agreement between the member states. Such an agreement would necessitate a mechanism of export quotas to minimize losses from competition and price volatility on the liberalized European market.

The GECF has not become a cartel; it remains merely a platform for discussion. Even though several initiatives have been proposed to resolve the economic problems faced by the gas industry by achieving a proper balance between the interests of consumers and producers, the forum has failed to take any meaningful steps in that direction. The participating countries have not managed to work out a coordinated position regarding the prospects for the development of the gas markets; without such coordination it will be difficult to avoid uncivilized competition.

In addition, the GECF Executive Board and the Secretariat have been too busy with organizational and technical issues, leaving them little time to develop a new gas price formation model which would take into account the environmental benefits of gas compared with other fossil fuels.

Also, the situation in the Middle East and North Africa remains extremely complicated, which indirectly affects the GECF. In recent months there have been signs of internal rivalry between such GECF members as Iran, Algeria, Qatar, and Libya—and that rivalry is set to grow.

On June 2, 2011 the GECF held its 12th ministerial meeting in Cairo. In a surprising twist, Qatar, where the GECF has its headquarters and where the organization held its first gas summit, failed to attend. Officials in Doha said there was a risk of an assassination attempt against Qatari officials by Libyan mercenaries at Cairo airport.

The reasons for such behavior seem twofold. First, the meeting in Cairo was attended by a Libyan representative who was a supporter of the Gaddafi regime. And second, there was uncertainty about the level of the officials who would attend the event (initially the meeting was supposed to be held at the level of heads of state or government). As a result, it was not clear who exactly would represent the member states at the Cairo meeting.

To summarize, there were serious disagreements between the participating states; not all the GECF leaders had agreed to attend the meeting; and the Egyptian hosts were extremely tardy with their preparations. There is little doubt that holding the 2011 summit in Cairo was a premature and ill-advised decision.

During the GECF Executive Board meeting in Qatar in February 2011 the participants decided to set up the High Level Ad Hoc Group for the 1st Gas Summit of the Gas Exporting Countries Forum. The group held four meetings; the present author was present at three of them as a member of the Russian delegation.

On the one hand, the Group's work had demonstrated the expectations of most of the GECF participants from the summit. They hoped that the event would provide a major impetus for the organization, and take it to a whole new institutional level. But on the other hand, it had become obvious that the participants lacked a consolidated stance. That lack of consolidation is probably the main obstacle to the organization's successful future.

The 3rd meeting of the high-level group was the first such meeting to be held in the absence of a quorum (two-thirds of the members). Of the 11 GECF members, only seven countries were in

attendance. Nigeria, Bolivia, Equatorial Guinea, and Libya failed to attend. The Libyan representative was denied a Qatari visa, which was a clear breach of the norms of behavior by the host country. The move was also at odds with the very spirit of an international organization such as the GECF, whose members are supposed to work in concert rather than undermining each other over their political differences.

Nigeria and Bolivia have not attended any of the recent GECF events; Bolivia is not even paying its annual membership fees. Equatorial Guinea is not showing any great interest in GECF activities either.

Nevertheless, the First Gas Summit of the GECF has taken place; the event was held under the headline “Natural Gas: the Answer to the 21st Century’s Sustainable Development Challenge.” But the level of the officials who took part in the event was not what is expected from a summit meeting.

Only a handful of countries were represented by their heads of state or government. The summit was attended by the Emir of Qatar, the President of Algeria (whose attendance had not been announced beforehand), and the President of Equatorial Guinea. Libya was represented by the head of its Transitional National Council. Russia sent the energy minister. The Russian senior leadership’s decision not to attend probably reflected the poor state of economic relations between Russia and Qatar.

The Iranian president, whose attendance was expected, changed his mind at the very last moment, sending his oil minister instead. There were several reasons for such a decision. First, two days ahead of the summit a GECF ministerial meeting decided to keep the current secretary-general in office for another two years, so the Iranians’ hopes of taking over that post were dashed. Second, the presence of members of the Russian leadership could have been used by some other participants to burnish their own international credentials—but the Russian president and prime minister decided not to attend. That may well have played a role in the Iranian president’s decision to cancel his own trip.

Qatar believes that although attendance was poor, the summit has helped to ensure the security of supply and demand on the gas markets; attract international attention to the environmental benefits of gas as an energy source; encourage investment in the gas industry; and give further impetus to GECF development.

The summit adopted a declaration which reflected the key objective of the event: to demonstrate to world producers and consumers of energy a consolidated position of the GECF states. The declaration also emphasized that natural gas, as the most effective and environmentally friendly fossil fuel, can and must become the basis for the development of GECF members, while at the same time serving the interests of all mankind. The document reflects the organization’s intention to develop ties with other consumers and producers of natural gas, as well as international organizations (such as the International Energy Forum). Further, the declaration speaks of the need to take into account the interests of the transit states and to create the conditions for the development and protection of cross-border infrastructure by the transit states and the consumers.

To summarize, the key objectives of the GECF in the immediate future are as follows: to complete the organizational shaping of the GECF and to begin its work in earnest; to continue strengthening the organization’s international positions; to pursue dialogue with the key players in the global energy market; and to attract new members.

Russia expressed its readiness to host the next GECF summit in 2013.

It has to be recognized, however, that for now the GECF has failed to live up to expectations. The existing long-term nature of Russia’s gas supply contracts with other countries, and the possibility of deeper cooperation in the framework of the Russia–EU Energy Dialogue—as well as cooperation with Japan, China, and other Asian countries—obviate the need for any gas export quotas. Such quotas would clash with the existing system of Russian gas supplies, which is based on long-term contracts. That is why it would make sense for Russia to abandon its lobbying for the GECF to become a “gas OPEC,” and to focus instead on furthering its national interests in the existing GECF framework.



RUSSIAN–QATARI GAS DIFFERENCES

Qatar's proven reserves of natural gas stood at 25.37 trillion cubic meters (14 percent of the world total) in 2011.⁸ By that indicator the country ranks second among OPEC members, and a global third after Russia and Iran.

Most of Qatar's gas reserves come from the offshore North Field. In geological terms, the North Field is a continuation of Iran's South Pars field; the two form one gigantic gas-condensate field.

It is worth noting that exploration of new gas reserves in Qatar was not very energetic until the early 1990s (see Figure 1). But the proven reserves figure began to grow rapidly in the middle of that decade. Annual gas production soon started to grow as well (see Figure 2).

In 2005–2010 Qatari gas output stood at just below 120 billion cubic meters. According to projections by Qatari specialists, the figure was expected to reach 160 billion by late 2012–early 2013,⁹ but these targets seem overly optimistic.

Looking at Figure 2, one can see that an increase in gas output by every 40 billion cubic meters has taken Qatar at least five years to achieve. In theory, the emirate could reduce that time to two years; after all, it has plenty of production capacity and access to the latest technologies. In practice, however, such a rapid increase is made impossible by the continuing moratorium on further development of the North Field.

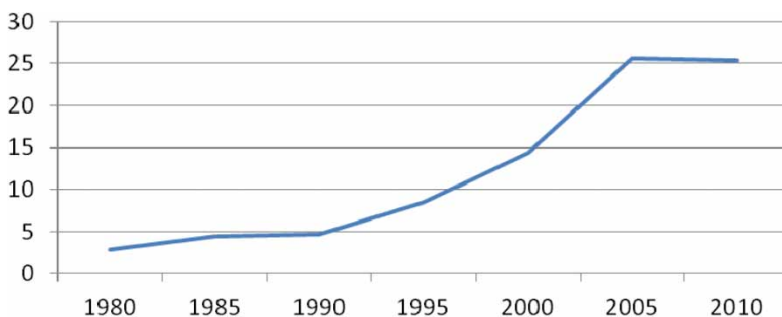
In all likelihood, Qatar does not actually harbor any illusions about its own abilities to increase production. The fact that it has voiced these overly ambitious targets should not be put down to lack of professionalism on the part of the emirate's industry analysts. It appears that Doha was merely trying to put information pressure on its LNG export competitors.

Growing production has enabled the country to increase its exports of liquefied natural gas (LNG).¹⁰ In 1996–2009 Qatari LNG exports accounted for 1.3–17 percent of global exports;¹¹ in subsequent years the figure showed very rapid growth. In 2010 there were 18 countries in the world which directly exported LNG; another four were involved in re-exports. Qatar was an undisputed leader among those 22 nations, with 25.6 percent of the global LNG exports figure.¹² The three runners-up—Indonesia, Malaysia, and Australia—accounted for 29.3 percent between them (see Figure 3).

In 1985–2005 the top spot in the global ranking of LNG exporters was held by Indonesia; Qatar claimed that spot in 2006. Between 2006 and 2010 the emirate increased its exports by more than 150 percent.

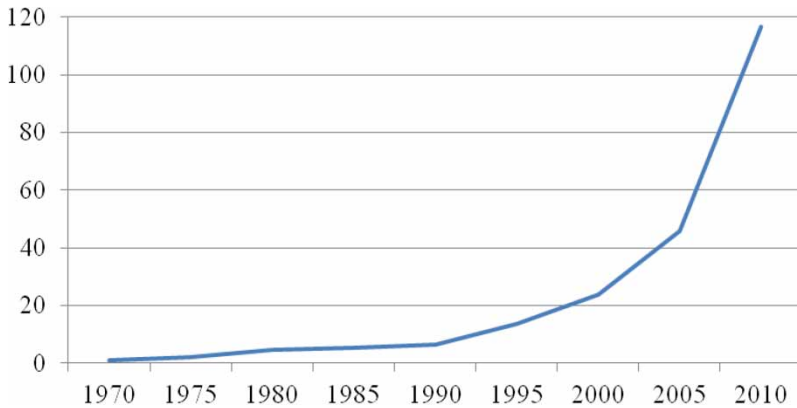
The rapid increase in Qatar's importance as a gas exporter has been made possible by a rapid development of infrastructure, spurred by favorable conditions in the regional markets and a healthy growth of demand for LNG prior to the onset of the world economic crisis in 2008. After launching a great deal of new production capacity, by 2010 Qatar had increased its annual LNG output to 77 million metric tons.¹³ The country had also laid the foundations for increasing that figure to 90–95 million metric tons, which was achieved the following year.

Figure 1. Qatari Proven Gas Reserves in 1980–2010 (Trillion Cubic Meters)



Source: BP Review of World Energy, 2011.

Figure 2. Qatari Gas Production in 1970–2010 (Billion Cubic Meters)



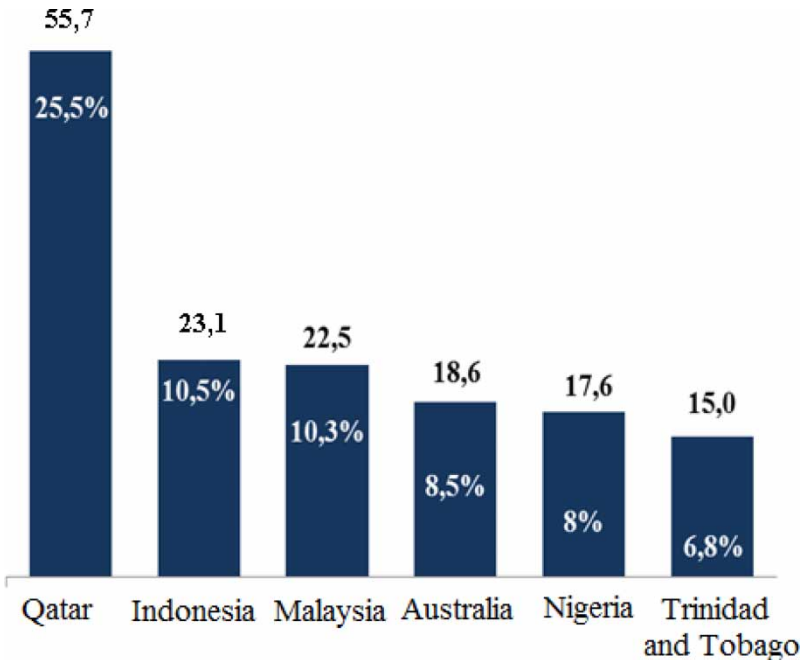
Source: BP Review of World Energy, 2011.

Specialists have calculated that the 10.1-percent increase in global LNG supply in 2011 can largely be attributed to growing Qatari exports, which rose by 34.8 percent compared with 2010. That increase accounted for 87.7 percent of the global exports growth figure.¹⁴

In 2011 Qatar exported 102 billion m³ of LNG. Most of those exports were destined for Asian and European markets (48.6 and 43.4 billion, respectively). The rest went to North America (6.5 billion), Central and South America (1.7 billion), and the Middle East (2.4 billion).¹⁵



Figure 3. Leading LNG Exporters in 2010 (Million Metric Tons and Percentage of World Exports)



Source: QNB Capital.

Qatar currently exports its LNG to over 20 countries.¹⁶ Over the past decade it has managed to diversify its export destinations significantly. Qatar has several longstanding Asian customers—Japan, South Korea, India—which have been steadily increasing their imports year on year. That is entirely understandable from the geographic and strategic point of view, and also taking into consideration that the demand for energy in many Asian countries is very high. But in recent years there has also been a significant increase in Qatari exports to Europe, including Britain (which is the largest importer of LNG from Qatar), Italy, France, Belgium, and Spain (see Figure 4).

Imports from Qatar account for more than a quarter of the European Union’s LNG consumption.¹⁷ Poland is currently building a new LNG terminal, scheduled for completion in 2014 (although the date may be brought forward). Initially it will receive more than 1 million metric tons of LNG from Qatargas,¹⁸ with plans to increase that figure by 2017–2018. Qatar is also in talks about LNG supplies with the Baltic states, Belarus, and Ukraine.

Germany says it is well aware of Qatar’s importance as a state which controls the world’s third-largest reserves of natural gas. The two countries have discussed LNG supplies and are very close to reaching an agreement; only logistical issues have yet to be sorted out.

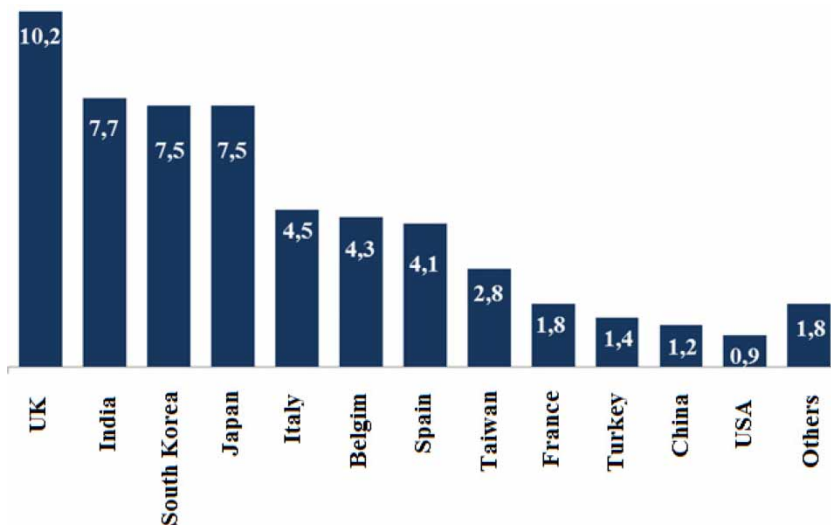
It appears that, initially, Germany will use the LNG terminal at the Dutch port of Rotterdam.¹⁹ In future, however, it intends to launch its own regasification terminals in Wilhelmshaven and Rostock.²⁰

German companies are already an important part of the Qatari oil and gas industry. The German oil and gas giant Wintershall has been involved in offshore exploration in Qatar since 1997. The GEA concern has won a Qatari contract to supply high-tech conditioners used in the oil and gas industry. Süd-Chemie, another German company, has signed a contract to build an LNG catalyst production facility in the Qatari city of Mesaieed.²¹

At first glance, it seems obvious that Qatar’s growing LNG exports to Europe will create difficulties for Gazprom because Europe is the main consumer of Russian gas. But according to an assessment by Russia’s Energy Minister Sergey Shmatko, which he voiced in the autumn of 2011, the emirate will not substantially increase its exports to Europe in the medium time frame.²² The minister stressed, however, that no firm commitments have been undertaken in that regard.

Qatar insists that its export policies are based on long-term contracts and on linking the price of gas to the price of oil. But, based on its own economic interests, the emirate is free to change the

Figure 4. Largest LNG Importers from Qatar in 2010 (Million Metric Tons)



Source: QNB Capital.

prices it charges to its customers and the destinations of its exports depending on the market situation.

Many of the existing assessments of Qatar's role in the European gas market are greatly exaggerated. Of course, imports from Qatar reduce the competitiveness of Russian gas supplies to Europe—but only to a small degree.

According to projections by Gazprom specialists, in the long term the gap between Europe's own gas production and consumption will grow, opening up new opportunities for imports—including imports from Russia.²³

The continent's dependence on gas imports is expected to increase, although Europe has a chance to diversify the sources of its gas supplies by increasing imports of Qatari LNG and reducing imports from Russia.

Once Qatari gas output increases following the lifting of the North Field moratorium in 2014, and once new LNG terminals have been launched in Europe, Qatar will become a much more important player in the European market, with far greater repercussions for Russian interests on the continent.

Russian industry analysts believe that over the next few years Qatar will supply an additional 50 billion m³ of gas to Europe every year, which constitutes 5 percent of the EU gas market.²⁴

Meanwhile, a rapid increase in shale gas production in the United States²⁵ has sharply reduced American demand for Qatari LNG. The United States is trying to achieve self-sufficiency in oil and gas; as a result, it has significantly reduced imports of hydrocarbons.

The Qataris have already built several large LNG plants,²⁶ which were intended to serve the American market (some of the Qatari supplies were meant to replenish the strategic fuel reserves at depots along the Gulf of Mexico coast). Now the Qatari LNG plants will work for the European market instead.

All of this will spur rapid growth of the Qatari economy, and attract an influx of foreign investment.

Let us look at the long-term LNG contracts Qatar has signed over the past decade (see Table 2).

It is clear from Table 2 that an increase in Qatari LNG exports to some destinations occurred before the launch of the corresponding additional production capacity. This means that new entries will appear in the existing list of contracts in the short and medium time frame, and that some of the new production capacity may replace the facilities which are reaching the end of their service life.

State-owned Qatar Petroleum plays a leading role in the country's oil and gas production—but the emirate cooperates closely with large foreign companies (mostly American ones), which can offer the latest technologies (see Table 3).

Table 3 demonstrates that Qatar is pursuing joint projects with foreign companies not only in developing new fields, but also in launching new gas and oil processing facilities. The emirate has set up two specialized state-owned companies for LNG exports: Qatargas²⁷ and Rasgas²⁸. The former currently controls 15 percent of the global LNG market.

Qatar is also working to roll out new gas-processing technologies. It was the first country in the Middle East to start making LNG by catalytic conversion (rather than the traditional refrigeration method) at its Oryx GTL plant. The facility can produce 34,000 barrels of products with extremely

Table 2. Qatar's Long-Term LNG Contracts in 2002–2012 (Million Metric Tons per Year)

Country/facility	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012
Japan/ <i>Qatargas</i>	6.7	6.7	6.7	6.7	6.7	6.7	6.7	6.7	7.5	7.5	7.5
South Korea/ <i>Rasgas</i>	4.8	4.8	6.8	8.8	8.8	8.8	6.8	4.8	7.5	7.5	7.5
India/ <i>Rasgas</i>	–	–	2.5	5.1	7.5	7.5	7.5	7.5	7.7	7.7	7.7
Italy/ <i>Rasgas 2</i>	–	–	–	–	–	4.7	4.7	4.7	4.5	4.5	4.5
Spain/ <i>Qatargas</i> , <i>Rasgas 2</i>	1.4	1.4	1.4	2.0	2.2	2.2	2.2	2.2	4.1	4.1	4.1

Source: Data supplied by the Qatari Embassy in Washington.



Table 3. Qatar's Oil and Gas Projects in 2005–2011

Project/field	Project type	Operator	Launched
KG	New development	Exxon Mobil (EM)	2005
Al Khaleej	Increasing production	Qatar Petroleum (QP)	2005
Dolphin	New development	QP, Total	2006
Oryx GTL	New development	Sasol	2006
Al-Seef LAB	New development	QP	2006
Rasgas 4	New development	QP/EM	2005
Rasgas 5	New development	QP/EM	2006
Rasgas 6	New development	QP/EM	2007
Rasgas 7	New development	QP/EM	2008
Id Al Shargi N.D.	Increasing production	Occidental Petroleum	2007
Ras Laffan	New development	QP	2008
Qatargas 4	New development	QP/EM	2007
Qatargas 5	New development	QP/EM	2008
Qatargas 6	New development	QP/EM	2009
Qatargas 7	New development	QP/EM	2010
AKG (new phases)	Increasing production	QP/EM	2008
Maydan Mahzam	Increasing production	QP, Total	2008
Al Rayyan	Increasing production	Anadarko Petroleum	2008
Al Shaheen	Increasing production	Maersk	2009
Perl GTL. Phase I	New development	Shell	2009
Perl GTL. Phase II	New development	Shell	2010
Exxon Mobil GTL	New development	EM	2011
Oryx GTL	Increasing production	Sasol	2011

Source: Qatar Petroleum, Qatargas, Rasgas.

low sulfur content, including 24,000 barrels of diesel, 9,000 barrels of naphtha, and 1,000 barrels of the propane–butane mix known as liquefied petroleum gas (LPG).²⁹ The diesel is exported mainly to Europe, naphtha to the Far East, and LPG is sold on the domestic market. The plant, which is worth an estimated 1 billion dollars,³⁰ is co-owned by Qatar Petroleum (51 percent) and Sasol (49 percent).³¹

Compared with other energy projects, the LNG industry requires a lot of investment, huge land plots for industrial development, and a large guaranteed supply of natural gas for a period of at least 20 years.

Qatar is able to meet all these requirements. An even larger Qatari project is the Perl GTL plant in the town of Ras Laffan. It is the world's largest facility to use the latest gas-to-liquids technology. Launched in 2011, the plant is owned by Qatar Petroleum (which owns a 51-percent stake) and Royal Dutch Shell (49 percent). The facility is already operational, and first shipments to consumers have already been made. It is expected to reach its maximum daily output of 140,000 barrels of natural gas fuel by 2013.

In addition, the plant will produce 120,000 barrels a day of oil equivalent in natural-gas liquids and ethane. The Perl GTL project was initially expected to cost 4 billion dollars—but the figure may well spiral to 18–19 billion.³² Nevertheless, the project demonstrates Qatar's determination to diversify its gas processing industry, which should further strengthen the country's energy exports.

With its constantly growing production capacity, Qatar is well placed not only to strengthen its global leadership in LNG exports but also to become the region's most powerful player on the market for natural-gas liquids.

CONCLUSIONS AND PROJECTIONS

In the short to medium term, Qatar will further increase its investment in the gas industry because gas export revenues are crucial for the continued well-being of that country's economy.

According to projections, in the 2030 time frame Asian demand for natural gas will grow at an annualized rate of 4.6 percent³³—faster than anywhere else in the world. China will account for 23 percent of the increase in global demand by 2030.

The commensurate increase in supply will be generated primarily by the Middle East (26 percent), especially Qatar. That assumption is based on the projection that LNG production will grow at a faster pace than global gas production or exports via pipelines. The share of LNG in the global increase of supply in 2010–2030 will constitute 25 percent (compared with 19 percent in 1990–2010).

Some researchers say that as a result of the global economic crisis the growth in European demand for LNG has slowed³⁴; that, however, is hard to believe, given all the new projects to build regasification terminals on the continent.

Also, many Russian and foreign experts are predicting that the burgeoning shale gas industry in the United States³⁵ will turn that country into an LNG exporter.³⁶ Such predictions seem premature; first we have to wait for the decision of the U.S. Environmental Protection Agency, which may well halt shale gas production for environmental reasons. Nevertheless, the United States is already close to self-sufficiency in gas thanks to its growing shale gas output.

There is, however, a strong impression that all the talk of the shale gas revolution is merely an attempt to cause panic among exporters, and to force them to reduce energy prices because currently the struggling U.S. economy cannot afford the high price of hydrocarbons. In 2011 Standard & Poor's, an international credit rating agency, set a precedent by reducing the United States' sovereign debt rating from the maximum level of AAA to AA+.³⁷ The move was triggered by concerns over the U.S. budget deficit.

Over the coming 20 years oil will be the slowest-growing energy source. Nevertheless, the demand for liquid fuels (oil, biofuels, etc.) will probably increase by 16 million barrels a day, thanks mainly to growing demand in large Asian countries, especially China and India.³⁸ OPEC will retain its position as the main supplier, with Saudi Arabia, Iraq, and Libya as the biggest exporters.

In the longer term we should expect growing exports of Qatari hydrocarbons (mainly LNG, and, to a lesser extent, oil) to Europe, Asia, and the United States.

An important advantage Qatar has on the LNG market is the latest technologies used by its companies. These technologies reduce costs and provide for greater efficiency during production, transportation, and regasification.

The introduction of new know-how has helped Qatar to launch additional production capacity and to achieve economies of scale. The annual output of its largest LNG facilities has reached 7.5–8.0 million metric tons.

Substantial progress has also been achieved in transportation technologies. The acquisition of the new Q-Flex and Q-Max LNG tankers, which are very large and have the equipment to convert boil-off gas into LNG, has enabled Qatar to cut costs and reduce gas losses during transportation.³⁹

Speaking about the projected increase in Qatari LNG exports to Europe, we should not forget that Moscow can take some steps to stymie those plans. More specifically, it can slightly reduce the prices it charges European consumers for natural gas delivered via pipelines, while also increasing the volume of its exports.

In the longer time frame Qatar is unlikely to shift its economic priorities to Europe. It has always been more interested in partnership with the Asian countries, which have a huge potential for economic growth. That growth will translate into many decades of high demand for energy—including energy supplies from Qatar.

Economic cooperation between Qatar and the leading Asian countries is growing at an exponential rate. This is largely due to the geographic factor—but the relative proximity of the emirate to its Asian markets is not the only thing that helps. Several other factors are also at play here.

First, Asian demand for energy is very strong, and continues to grow in line with these countries' rapid and sustained economic growth.



Second, the Qataris share the Asian business culture, with its emphasis on spoken agreement, mutual trust, and respect between the partners, as opposed to formal written commitments and rigid adherence to the norms of legislation.

Third, the relatively small and compact emirate has earned itself a good reputation and is able to pursue its ambitious goals because for some Asian countries that are much larger and more populous than Qatar the emirate is one of their main trading partners.

Judging from the Qatari trade figures over the past years and decades, the Asian countries have been filling the emirate's coffers for many years now—whereas trade with Europe took off in earnest only after 2009.

Qatar will probably continue to strengthen its position on the European markets by gradually increasing its exports and investment—not as an alternative to Asia, but as a hedge against unforeseen problems in its key market, and as a way of securing additional revenue to pursue ambitious domestic projects.


Compared with Qatari trade with Europe and Asia, economic cooperation with Russia leaves much to be desired. There are three main reasons for this. First, there is the deteriorating political climate between the two countries following the change of regimes in some Arab states in 2011. Second, many of the Western managers working for Qatari businesses have adopted a clearly anti-Russian stance. And third, there is a certain degree of divergence between the Russian and Qatari business mentality.

The strength of future economic contacts will depend, among other things, on Russia's official position on pressing Middle Eastern problems, as well as on Qatar's own political profile.

The first of these two factors is by far the most important. Clearly, Moscow is unlikely to find a common language with the emirate if the Kremlin's statements and Qatar's policies in the region remain at odds.

The second factor is much less important, because Russia has tried to lay the foundations for bilateral investment cooperation despite the fact that Qatar's own reputation is not exactly stellar. For many years the emirate has provided financial and ideological support to extremist, terrorist, and separatist groups in other Arab countries. So this is certainly not the main consideration—but it must be taken into account as well.

The rapid economic growth achieved by Qatar in recent years underpins the country's ambitions of becoming not only the region's leading financial center but also a powerful player in the Middle Eastern and global arena in the broader sense. The country has a unique economic and geopolitical position, lying as it does on the crossroads between Europe, Asia, and Africa. Its large reserves of hydrocarbons also put it in a good position to pursue even closer cooperation with Western and Asian countries, which are all betting big on such cooperation.

As for Russia, effective trade and investment partnership between this country and Qatar is impossible because of the numerous political and economic differences. At the same time, it cannot be ruled out that at some point in the future the two countries will manage to resolve these differences and achieve a more or less acceptable level of bilateral economic cooperation. 

NOTES

¹ There have been several visits to Russia by senior Qatari officials, including the Emir, Sheikh Hamad bin Khalifa Al Thani, and the Prime Minister and Foreign Minister, Sheikh Hamad bin Jassim bin Jabor Al Thani. The list of Russian officials who have visited Qatar includes the Deputy Prime Minister, Igor Sechin, and the high presidential representative in the Urals Federal District, N.A. Vinnichenko. There have also been a number of visits to Doha by Russian delegations which included ministers, members of parliament, political leaders and public figures, and senior managers of large state-owned and private companies.

² "Structure of Russian foreign trade with Qatar," prepared by the Russian Ministry of Industry and Trade, February 2011, p. 3.

³ "Direction of Trade Statistics," IMF, 2010–2011.

⁴ According to the Qatari Statistics Department.

- ⁵ In 2011 analysts of Britain's Ernst&Young and the Oxford Economics Institute published a forecast for the development of fast-growing markets. Qatar was at the top of the rating, with average annual GDP growth at 13 percent in 2000–2013.
- ⁶ For several years the GECF included 11 member states: Algeria, Bolivia, Egypt, Equatorial Guinea, Iran, Libya, Nigeria, Qatar, Russia, Trinidad and Tobago, and Venezuela. Oman joined the organization after the 13th ministerial meeting held on November 13, 2011 in Doha. Kazakhstan, the Netherlands, and Norway have observer status. According to the GECF statute, Brunei, Indonesia, Malaysia, Turkmenistan, and the UAE are welcome to join whenever they wish; the five countries participated in the work of the forum back when it was an informal club. The GECF is also open for membership by any gas exporting country which shares its goals and objectives.
- ⁷ Author's interview with the head of Qatar Petroleum, Mohammed Al-Hajri. Doha, May 19, 2011.
- ⁸ CIA World Factbook 2012.
- ⁹ QNB Capital, *Qatar—Economic Insight, September 2011*, <<http://www.qnb.sy/csportal/BlobServer?blobcol=urlenglishdoc&blobtable=QNBNewDocs&blobkey=id&blobwhere=1316689058982&blobheader=application%2Fpdf>> .
- ¹⁰ Liquefied natural gas (LNG) is produced from natural gas by refrigeration or high pressure. Liquefaction allows easier and more compact storage and transportation to the consumer. The specific weight of LNG is about half the figure for petrol. Its boiling point is from –158 to –163 degrees Celsius, depending on the composition. The compression ratio for LNG is from 92 (the so-called environmental regime used at gas distribution stations) to 95 percent.
- ¹¹ *IGU World LNG Report—2010*, p. 7.
- ¹² *Ibid*, p. 6.
- ¹³ Qatari state-owned company Rasgas, <<http://www.rasgas.com/>>, last accessed January 27, 2013.
- ¹⁴ *BP Statistical Review of World Energy*, June 2012, p. 4.
- ¹⁵ *Ibid*, p. 28.
- ¹⁶ Until 2009 Qatar supplied its gas mostly to the markets which offered higher prices (spot contracts), enabling the emirate to receive additional revenue and to invest it in developing its LNG infrastructure. Nevertheless, every so often Qatar would supply gas under short-term contracts at prices below market, causing anger among other LNG exporters. In recent years the country ended that practice and transitioned to fixed-price medium and long-term contracts so as to avoid dumping charges.
- ¹⁷ RREEF Research, “Liquefied Natural Gas Market in Europe,” February 2011, <http://www.rreef.com/content/media/Research_Liquified_Natural_Gas_Market_in_Europe_Februar_2011.pdf>, last accessed January 27, 2013.
- ¹⁸ “Emir's Poland Visit Will Cement Ties: Envoy,” *The Peninsula*, October 14, 2011.
- ¹⁹ “The Polish LNG Terminal and Germany,” *Vokrug Gaza*, February 9, 2011, <<http://trubagaz.ru/issue-of-the-day/polskijj-spg-terminal-i-germanija/>>, last accessed January 27, 2013.
- ²⁰ Karel Schweng, “Verflüssigtes Erdgas—Ein Markt im Fokus,” *Die Materialsammlung der Fachtagung unter dem Titel “Erdgas Umwelt Zukunft,”* Leipzig, January 25, 2007.
- ²¹ “Süd-Chemie Starts Catalyst Production as the First Company in the Fast Growing Market in Qatar,” <http://www.sud-chemie.com/scmcms/web/page_en_7235.htm>, last accessed January 15, 2013.
- ²² The official's position is accurate as of November 2011.
- ²³ Gazprom corporate journal, No. 5 (2012), pp. 12–13.
- ²⁴ “Qatar's Plans Threaten Gazprom's Positions in Europe,” <<http://www.newsland.ru/news/detail/id/981878/>>, last accessed January 15, 2013.
- ²⁵ Natural gas consisting mainly of methane and produced from shale rock using horizontal drilling, hydraulic fracturing (fracking), and 3D GEO seismic modeling techniques.
- ²⁶ Qatar Petroleum (70 percent stake) and Exxon Mobil (30 percent) have launched the Rasgas 6&7 facility, which consists of two identical blocs, with a total annual capacity of 15.6m metric tons. Qatar Petroleum (68.5 percent), ConocoPhillips (30 percent) and Mitsui (1.5 percent) have launched the Qatargas 3 facility, with an annual capacity of 7.8 million metric tons. Qatar Petroleum (70 percent) and Royal Dutch Shell (30 percent) have launched Qatargas 4, which has the same capacity.



- ²⁷ The company was founded in 1980; it is a joint venture between Qatar Petroleum (65 percent), Total (10 percent), ExxonMobil (10 percent), Mitsui (7.5 percent) and Marubeni (7.5 percent) (the last two are Japanese companies).
- ²⁸ The company was set up in 2011 by Qatar Petroleum (70 percent) and ExxonMobil (30 percent).
- ²⁹ “Gas to Liquids,” Topic Paper No. 9, Working Document of the NPC Global Oil & Gas Study, July 18, 2007, <http://www.npc.org/Study_Topic_Papers/9-STG-Gas-to-Liquids-GTL.pdf>, last accessed January 15, 2013.
- ³⁰ “Oryx GTL and the GTL Sector,” *International Gas* (magazine of the International Gas Union), April 2007, p. 127, <<http://www.igu.org/knowledge/publications/mag/apr07/p126-150.pdf>>, last accessed January 15, 2013.
- ³¹ Qatar Petroleum has signed a memorandum with a joint venture of South Africa’s Sasol and Chevron on increasing the daily output of the Oryx GTL facility to 100,000 barrels, which will require huge investment.
- ³² “Pearl GTL—An Overview,” Shell, <http://www.shell.com/home/content/aboutshell/our_strategy/major_projects_2/pearl/overview/>, last accessed November 23, 2012.
- ³³ *BP Energy Outlook 2030*, London, January 2012, p. 31.
- ³⁴ M. Babaeva, *Transnationals on the Global LNG Market*, author’s summary of a PhD thesis (Moscow, 2010), p. 10.
- ³⁵ *BP Energy Outlook 2030*, London, January 2012, p. 34.
- ³⁶ Sberbank Rossii Center for Macroeconomic Studies, “Natural Gas: A Brief Review of the Global Industry and Analysis of the Shale Boom,” May 2012, pp. 3–4.
- ³⁷ See: Standard & Poor, Ratings, <<http://www.standardandpoors.com/ratings/articles/en/us/?assetID=1245316529563>>, last accessed January 15, 2013.
- ³⁸ *BP Energy Outlook 2030*, London, January 2012, p. 23.
- ³⁹ Babaeva, op. cit, p. 16.



THE FUTURE OF NON-STRATEGIC NUCLEAR WEAPONS IN EUROPE: OPTIONS AVAILABLE

What is the precise definition of non-strategic nuclear weapons (NSNW)? Should NSNW talks be held in bilateral or multilateral format? What would be more effective? And will the initiatives on NSNW reductions in Europe yield any tangible results? These and other questions have been discussed by: Lt-Gen (Rtd), PIR Center Senior Vice-President, Evgeny Buzhinsky; Senior Research Fellow of the Center for Arms Control, Energy and Environmental Studies (Moscow), Anatoly Dyakov; Acting Head of the Main Department for International Military Cooperation at the Russian Ministry of Defense, Evgeny Ilyin; PIR Center's Russia and Nuclear Nonproliferation Program Coordinator, Alexander Kolbin; Deputy Director for Science and Research at the Institute of Strategic Stability (Moscow), Viktor Koltunov; First Secretary of the Department for Security and Disarmament at the Russian Foreign Ministry, Mikhail Kustovsky; PIR Center President, Editor-in-Chief of the Security Index journal, Vladimir Orlov; Advisor to the Chief of the Russian General Staff, Alexander Radchuk; Senior Research Fellow at the Center for Arms Control, Energy and Environmental Studies (Moscow), Vladimir Rybachenkov.¹

EVGENY BUZHINSKY (PIR CENTER): The American and European proponents of Non-Strategic Nuclear Weapons (NSNW) reductions—especially reductions affecting the Russian NSNW arsenal—stepped up their rhetoric in 2010. The new Strategic Concept adopted by NATO at the Lisbon Summit in November 2010 and the U.S. Senate's resolution on the ratification of the New START treaty (December 2010) include paragraphs which allege “a disparity between the U.S. and Russian NSNW stockpiles.” It is not clear, however, why it is alleged that the Russian stockpiles are much larger; neither Russia nor the United States has ever published official figures about the numbers of non-strategic nuclear weapons in their arsenals.

NSNW: DIFFERENT APPROACHES

Western concerns about the Russian NSNW stockpiles boil down to two main arguments. First, in the event of a serious military conflict, non-strategic nuclear weapons deployed with conventional forces may be used at an earlier stage during the conflict, thereby increasing the risk of further nuclear escalation. Second, non-strategic nuclear weapons—especially older designs—are not equipped with reliable measures against unauthorized use; they are also compact, making them an attractive target for terrorists.

Neither of these two concerns has merit. On the first point, NSNW can be used against an aggressor only as a measure of last resort, in the event of a serious threat to Russia's territorial integrity and sovereignty; such use requires direct authorization from the Russian president. The second point is equally groundless because at present, all NSNW are being stored at central depots; they are equipped with reliable measures against accidental or unauthorized use. This is amply demonstrated by the fact that there has not been a single proven case of Russian nuclear ammunition being lost or stolen.



The definition of NSNW covers all nuclear weapons, with the exception of:

- ❑ strategic nuclear warheads for ICBMs and SLBMs, as well as nuclear bombs and cruise missiles deployed on strategic bombers, as defined by the New START treaty;
- ❑ nuclear ammunition which has been removed from central storage depots prior to being dismantled.

Although Russia has never released official figures about the size of its NSNW stockpiles, it is believed that Moscow has about 3,700–5,400 tactical nuclear weapons, of which 2,000 are ready for combat use. These include various types of cruise missiles, free-falling bombs, and torpedoes. The Russian NSNW arsenal has been reduced by at least 75 percent since 1991, from 15,000–27,000 weapons. In the 1990s all the remaining tactical nuclear munitions were moved to central storage depots.

NSNW play a uniquely important role in Russian military strategies. In the current situation, these weapons are almost the only guaranteed instrument for ensuring Russia's independence and territorial integrity in the event of a serious regional conflict.

The Russian nuclear forces have a twofold role, which consists of traditional nuclear deterrence and limited use to repel a massive conventional attack. Both of these tasks are reflected in the Russian Military Doctrine.

The main reason why Russia has long-range NSNW is because the United States and NATO have a large superiority in high-precision long-range conventional weapons. The Russian leadership is taking steps to correct the situation by acquiring a similar high-precision, long-range conventional capability. But until those steps have yielded results, Russia is forced to rely on limited use of nuclear weapons with a similar range.

The Russian Navy is especially reliant on NSNW because in accordance with the Russian Naval Doctrine until 2020, the Russian Navy is tasked with “protecting Russian territory from the sea, guarding and defending the Russian maritime borders and the airspace over those borders.” The number of ships and submarines in service with the Russian Navy has fallen substantially since the early 1990s. Also, we have to take into account the experience of recent military conflicts, during which the main strikes against targets on the adversary's territory were delivered by cruise missiles launched from ships and submarines, as well as by high-precision bombs dropped from naval aviation aircraft. That is why it is entirely justified for the Russian Navy to rely on NSNW.

Russia and the United States have very different reasons for needing their NSNW arsenals. For the United States and NATO, the value of those arsenals is primarily political; they help to strengthen the transatlantic security ties, and underpin NATO's nuclear capability. For Russia, however, the value of NSNW is primarily military. They help to neutralize the U.S. and NATO countries' superiority in conventional weapons; augment the fighting ability of Russia's conventional forces; and serve as an instrument for preventing an escalation of armed conflicts. What is more, Russia regards its NSNW as a deterrent against third countries which have nuclear weapons and delivery systems capable of reaching Russian territory. The latest reductions in Russia's strategic nuclear capability under bilateral agreements with the United States have also served to increase the role of the Russian NSNW arsenal, which is becoming an important instrument of deterrence against the Eurasian countries which possess nuclear weapons.

ANATOLY DYAKOV (CENTER FOR ARMS CONTROL, ENERGY AND ENVIRONMENT STUDIES): I would like to comment on Gen. Buzhinsky's remark about the definition of NSNW. Let us imagine, in purely hypothetical terms, that someone has used a nuclear weapon. I think it will not make much of a difference whether the weapon in question was tactical or strategic—the event itself will be on a strategic scale. We should all be clear about it. That is why the distinction between strategic and tactical nuclear weapons is largely artificial.

We are essentially discussing the situation between the United States and Russia. In this context, I would offer the following definition of NSNW. My colleagues and I at the Center for Arms Control, Energy and Environment Studies define non-strategic nuclear weapons as U.S. and Russian nuclear munitions designed for delivery systems which are not covered by bilateral arms control and reductions agreements. Of course, such a definition cannot be used for third countries' nuclear weapons.

MIKHAIL KUSTOVSKY (RUSSIAN FOREIGN MINISTRY): The Russian Foreign Ministry has noted increased interest in NSNW-related issues on the part of European countries. Various initiatives and proposals have been voiced, with a whole set of demands addressed primarily to Russia. Calls have been made for reducing the existing stockpiles of NSNW, ensuring transparency, disclosing the location of the storage depots, etc. A similar approach is used in the documents adopted at the 2010 NATO summit in Lisbon.

Russia is open for discussion of any issues related to international security. But we do not see the NSNW problem as a priority. In the area of arms control, efforts should focus on the following areas: unilateral steps to deploy a global missile defense system; plans to develop strategic delivery systems armed with conventional warheads; the threat of weapons being placed in outer space; the existing imbalance in conventional weapons; etc. Efforts to maintain strategic stability should be carefully thought out, and they should be made step by step. At this point it is important to see how the New START treaty between Russia and the United States performs, and how the norms and understandings contained in that treaty are being implemented.

As for NSNW, as part of the presidential initiatives announced in 1991–1992, Russia has reduced its NSNW arsenal by three-quarters. All non-strategic nuclear weapons have been moved to the non-deployed category and removed to central storage depots on Russian territory. Meanwhile, the United States still has its nuclear weapons capable of reaching Russian territory deployed in Europe. Since 1996 we have repeatedly urged other nuclear-weapon states to follow our example by removing NSNW to their national territory and by completely dismantling the nuclear weapons infrastructure on other countries' territory, thereby making it impossible to deploy those weapons at short notice. A constructive discussion of the NSNW problem would be facilitated by ending the practice of military exercises which involve NSNW and in which non-nuclear-weapon states take part. A decision by NATO countries to relinquish the concept of joint use of nuclear weapons would be another useful step in that direction. The new NATO Strategic Concept adopted on November 19, 2010 at the Lisbon summit essentially retains the old Cold War-era approaches.

Before we begin to discuss the NSNW issue, it would be useful to do some preparatory work. First and foremost, we need to produce a universal classification of NSNW, and to develop a shared set of definitions. Different countries use different definitions for similar weapons; they describe them as tactical, non-strategic, sub-strategic, pre-strategic, etc. That is especially important because some weapons types, such as air bombs, can be categorized as strategic as well as non-strategic weapons. In other words, it will be difficult to continue further dialogue unless we first resolve the issue of definitions.

Another thing I would like to stress is that not only the United States and Russia, but other countries as well have NSNW in their arsenals. At this point, these countries are not showing any signs of being ready to discuss the problem and to join the nuclear disarmament process. Russia believes, however, that further progress on nuclear disarmament, including NSNW reductions, will be very difficult to achieve without making that process multilateral.

VIKTOR KOLTUNOV (INSTITUTE OF STRATEGIC STABILITY): I believe that certain conditions must be put in place first. There must be a willingness to address the missile defense problem; to set up, at the very least, a working group on outer space at the Conference on Disarmament; and to enter into force the adapted Conventional Armed Forces in Europe Treaty (CFE). At the very least, there must be some signals. Right now, there are no such signals. We must begin addressing the question of further nuclear disarmament steps by holding consultations. These consultations must be in a multilateral format—I disagree with the view that they should involve only Russia and the United States.

I believe that these consultations should aim to produce a mandate for future talks, once the conditions for such talks have been put in place. We already have a precedent: the CFE talks began from a mandate. The mandate for NSNW talks should answer many important questions. First, it is the question of what kinds of weapons should be cut. Attempts to produce a definition for tactical weapons are pointless; coming up with a universal definition is an impossibility, and for several reasons. The same weapons type can be tactical in one set of circumstances, but strategic in another, in a different combat theater. So we should either be talking about all nuclear weapons—or, to follow the example of the INF talks, we should categorize nuclear weapons by indices, etc. Another important question that must be answered is the new levels to be achieved after the reductions.



ALEXANDER RADCHUK (RUSSIAN GENERAL STUFF): The NSNW problem is very multi-faceted. No problem related to nuclear weapons—and especially nuclear arms reductions—has ever been resolved separately from the general political and geopolitical context. Let us recall, for example, that non-strategic nuclear weapons deployed in Cuba became a strategic nuclear factor—after which we began to make progress towards Helsinki, the SALT treaty, and the START treaties. As soon as we had agreed some specific figures, we started making specific nuclear plans and calculations. After the figures, there were questions of usage and application, there were efforts to calculate the number of Pershing missiles to be deployed in Europe, or the number of the Pioneer missiles Russia must deploy in response—in other words, there was a balancing act. It became clear what specific figure is needed for specific nuclear planning.

Does Russia need to pedal the NSNW situation? Let us see. There is a huge nuclear talks lobby, which will be twiddling its thumbs for the next 10 years now that the New START treaty has been signed. What are these people to do now? These are all very respected and reputable people. So what is it about NSNW that worries them so much? If we are talking about NSNW in Europe, then we have already established that these weapons are not covered by the New START treaty. France and Britain are not covered, either. But we are talking about NSNW in the United States–Russia format. In that case, is it NSNW in Europe people are so worried about, or in Russia? I have the impression that it's the NSNW in Russia.

What, then, is the problem? To independent and unbiased experts, the answer is clear. Maybe there is some problem than we are not being told about, but if we start to analyze that problem, it will immediately become clear why. The very fact that we have NSNW is the actual problem. And if we start to discuss the problem of Russia having nuclear weapons, then let us recall that Russia is not only a European country. Half of our country is in Asia. It is the question of the Nuclear Nine. As soon as we start talking about Russian NSNW, we are immediately faced with the problem of all the other nuclear-armed countries. They will inevitably have to be part of any agreement, too.

HOW TO DISCUSS THE PROBLEM?

VLADIMIR ORLOV (PIR CENTER): Let me point out that NATO is very reluctant even to discuss the notion that nuclear weapons, regardless of their specific type, should not be deployed outside national territory. In early February the EU held a large conference in Brussels, a conference of the so-called EU Non-Proliferation Consortium. The NSNW issue dominated during some of the sittings held as part of that conference—and some of the opinions voiced were diametrically opposed.

One of the leading security experts, Lord Hannay of Chiswick, a member of the British House of Lords and formerly a senior British diplomat, said that the NATO Chicago Summit (which took place in May 2012) should approve a decision to withdraw NSNW from Europe without any preconditions or provisos, because these weapons are militarily useless and politically counter-productive. To which the head of the NATO WMD Center replied that nothing of the sort should be expected of the Chicago summit. The timing for such a move was not good at all; a change (or potential change) of president in at least three nuclear-weapon states in 2012 was expected, so 2012 was not the best time to raise such an issue.

I believe that we need to hold a serious discussion of the NSNW issue with our European partners.

VLADIMIR RYBACHENKOV (CENTER FOR ARMS CONTROL, ENERGY AND ENVIRONMENT STUDIES): Is the removal of American NSNW from Europe a realistic possibility? The paradox is that many U.S. military specialists believe the presence of tactical nuclear weapons in Europe does not offer any benefits. For example, Gen. James Cartwright, the [former] Vice-Chairman of the Joint Chiefs of Staff, recently said that U.S. tactical nuclear weapons in Europe do not serve any real purpose that is not already being served by strategic forces. Also, amid continuing U.S. defense spending cuts, and in view of the shifting defense priorities, with nuclear proliferation and nuclear terrorism seen as the key threats, the importance of tactical nuclear weapons is diminishing.

Nevertheless, there are still people in the U.S. establishment who believe that NSNW must be kept as a means of preserving transatlantic ties, and, more importantly, as a means of satisfying the requirements of the new NATO members. That is especially true of the small Baltic states, which believe that relinquishing U.S. tactical nuclear weapons in Europe is a red line which must not be crossed.

Russian–U.S. relations are beginning to deteriorate. The reset is over. In such a situation, there is no point discussing a new round of talks on arms reductions. Gen. Miller, the former deputy defense secretary, and Ted Warner, who was a deputy of Rose Gottemoeller at the disarmament talks, have said very clearly that the removal of tactical nuclear weapons from Europe is out of the question. And there is no reason to believe that this issue will be resolved in Chicago.

DYAKOV: Whether we like it or not, for historical reasons—due to the fact that the United States has a concept of “extended deterrence”—some of the U.S. tactical nuclear weapons are deployed in Europe. That is why it is safe to say that there are three parties in these talks. But NATO has 28 member states, so that gives you an idea of how many participants there are, potentially. Is it worth entering into talks with so many participants?

The process of strategic arms reductions is now under way, and that is a clear necessity. Sooner or later there will come a point when the number of tactical nuclear weapons will be about the same as the number of the remaining strategic nuclear weapons. Whether we want it or not, we will have to put NSNW on the agenda of the talks.

What are the American interests in this situation? I have recently reviewed a rather old but fundamentally important paper, the 2009 report by Karesh-Leging, which essentially laid the foundations of the latest U.S. Nuclear Posture Review. The report often refers to NSNW. In particular, it argues that the United States must keep track of the Russian tactical nuclear weapons because Russia has some high-precision weapons—namely, the short-range Iskander missiles. Using Iskander missiles with nuclear warheads gives Russia new capabilities for threatening the use of nuclear weapons in order to influence regional conflicts. But the report admits that Russia has to rely on NSNW owing to the existing imbalance in conventional weapons. This is quite a serious piece of work, although not all of its proposals have made it to the Nuclear Posture Review. Hence the conclusion which was made by the Republicans during the discussion and ratification of the New START treaty, i.e. the conclusion that NSNW must be on the agenda during the next round of the talks.

The already mentioned Senate resolution on the ratification of the New START treaty says that the U.S. administration should seek the inclusion of NSNW on the agenda of the next round of talks on arms reductions, and that deployed and non-deployed nuclear weapons should be discussed as a single package. For a long time we have been debating the issue of the American break-out potential. In essence, we were talking not about cuts but about reducing the level of combat readiness, whereby the warheads are removed but the delivery systems still remain. The Americans are proposing more or less the same thing, i.e. the delivery systems still remain. So if we discuss reductions, it will mean that the Russian capability is reduced. Such a reduction jeopardizes the strategic parity which currently exists, and which Russia has always aimed to preserve.

As for the Russian position, speaking at the Munich conference in 2011, then Russian Deputy Prime Minister Sergey Ivanov said that, on the whole, we accept that the NSNW problem will have to be discussed—but on several conditions. These conditions have already been outlined during our discussion today. Let me add one more condition. I think that the conditions should include the fact that actually we need to think about building a new security architecture in Europe. Russia has already made proposals to that effect—but the Western reaction has been lukewarm.

As a result, right now there are no reasons for us to enter into talks or consultations on the NSNW issue. In 2004 we worked on a study which focused on NSNW—and back then we arrived at the same conclusion.

ORLOV: I would like to draw your attention to one notion voiced today—the notion that the issues we are discussing today, including the NSNW issue, could be addressed in the broader context of a new security architecture in Europe. Russia’s first attempt, which was announced by Dmitry Medvedev—the European Security Treaty proposal—has not been successful. Maybe we have not done everything we could have, but as of today no progress has been made. The old European security architecture does, on the whole, need replacing. And the mechanism of replacing it should not be limited to purely military issues.

ALEXANDER KOLBIN (PIR CENTER): The conditions for launching talks on NSNW reductions in Europe are not yet right. The United States believes that the latest conventional weaponry will make it less reliant on nuclear weapons. Russia, meanwhile, is responding to America’s break-neck progress in the development of new conventional weaponry by increasing its reliance on nuclear weapons.



Based on that logic, Russia will have to meet many more conditions before beginning the talks. In the meantime, the United States is not only putting forward conditions, but also energetically discussing at the level of experts several possible approaches to future reductions. When the time comes for negotiations (and I have no doubt that it will), Russia may well find that it has fewer options to choose from.

On the whole, even though our position on NSNW lacks transparency, if we analyze those few public statements that have been made by our civilian and military leadership, we can conclude that Russia's conditions are as follows.

First, any future disarmament talks which involve nuclear weapons must also take into account a whole set of other problems. They cannot be held in isolation from a much broader context which currently includes the problem of militarization of space; the problem of the deployment of a global missile defense system by the United States; the modernization of the CFE regime; the problem of strategic non-nuclear weapons and high-precision weapons; and disparity in conventional weapons. Moscow can never accept a deal whereby in return for the removal of 200 U.S. nuclear bombs from Europe, Russia will have to cut or remove from the European part of its territory the much larger Russian NSNW arsenal.

Second, it has repeatedly been said in Russia that before entering into any talks on the NSNW issue, we must see the completion of the implementation of the New START treaty. That means that the talks cannot begin before 2018. By that time Russia will probably be even less inclined to discuss NSNW than it is now, owing to several developments. These include the expected completion of the fourth phase of the deployment of the U.S. missile defense system in Europe; the replacement of the F-15 and F-16 bombers currently in service with the U.S. Air Force with the more advanced F-35 model; and the completion of the program to extend the service life of the B-61 bombs.

Third, other nuclear-weapon states besides Russia and the United States must also take part in the talks. There are two nuclear-weapon states in Europe, France and Britain. France has what amounts to non-strategic nuclear weapons, but it says that those weapons are actually strategic. Britain also says that it does not have any NSNW in its arsenals. Another demonstration of the fact that the two countries have no intention of putting any part of their nuclear arsenals up for NSNW negotiations was the 2008 European plan for nuclear disarmament. The document has been signed by all 27 EU members. It clearly states that before multilateral (rather than bilateral) nuclear disarmament can be put on the agenda, lower levels of nuclear weapons must be reached in the framework of bilateral Russian–U.S. talks, and that NSNW must also be subject to future reductions. New issues may also emerge in connection with the gradual integration of the French and British nuclear forces, which was announced in late 2010.

Finally, the most important condition is that the United States must withdraw its NSNW from Europe and dismantle all the requisite infrastructure. Of course, our concerns about the infrastructure are not groundless. The NATO 2020 report, which was written by a group of experts in 2010 as part of preparations for adopting the new NATO Strategic Concept, said that any changes in the NATO nuclear policy, including decisions on the geographical distribution of the alliance's nuclear weapons in Europe, must be authorized by NATO as a whole. In the end, that phrase did not appear in the text of the Strategic Concept adopted in Lisbon. But it does run counter to the 1997 Founding Act on Mutual Relations, Cooperation and Security signed by Russia and NATO, which says that NATO has no intentions, plans, or reasons for deploying nuclear weapons on the territory of the new members of the alliance.

As for the United States, first, Washington does not link NSNW reductions to modernization of the CFE or the removal of its NSNW from Europe. Neither does it want to include the nuclear disarmament problems in the overall disarmament agenda. Also, for now—officially at least—the United States is talking only about bilateral consultations with Russia. As for the Russia–NATO talks, the Americans believe that the agenda of any such talks should not include French or British nuclear weapons. The only thing Washington is prepared to do is to hold consultations on the NSNW issue with its allies.

On the whole, we can assume that the Americans will probably remove their NSNW from Europe in a gradual fashion, while at the same time increasing transparency with regard to the numbers of those weapons, their deployment locations and deployment status—up to the point of removing those weapons completely. For now, the position adopted by the United States is less rigid than Russia's position. It says that Russia must remove its NSNW farther inland, away from the borders

with the NATO countries, before the American NSNW can be removed from Europe; nevertheless, the American NSNW are already being removed from Europe. This is already happening. It is believed that in 2000–2006 Washington removed nuclear weapons from Greece and from the Ramstein base in Germany, followed by the removal in 2008 from Britain. The military value of NSNW is not at all obvious. The American and British strategic nuclear arsenals can take care of all potential NSNW targets; NATO's non-nuclear deterrence capability in Europe is growing all the time; and NATO's borders have been pushed back eastwards.

People often ask the question of whether NSNW are a stronger bargaining chip for the United States or for Russia. Clearly, the United States is in a stronger position in that regard because it does not lose anything in terms of its own security by removing NSNW from Europe—the Americans themselves are saying this out loud. Russia, however, becomes more vulnerable in terms of security by reducing its NSNW arsenal. The latest demonstration of that fact is the article by Vladimir Putin on the subject of the Russian defense industry, and the statements he made in Sarov on February 24.

It appears that the most we can reasonably hope for at this moment is “talks about launching the talks.” A lot of work needs to be done to develop a common set of definitions. There are no simple or easy ways of resolving the problem of NSNW reductions and liquidation. We need to come up with the definitions, to develop control mechanisms, etc. No information exchange can be very successful without verification mechanisms. In any event, controls can work only if there is mutual trust.

There are several steps that could be undertaken in the immediate future. First, talks must begin between Russia and the United States—that is the most important thing, especially since at the first stage this is a problem for Russia and the United States, a problem of their NSNW on the European continent. Besides, if we try to make the talks multilateral from the very beginning, this will make it more difficult to develop control mechanisms and confidence-building measures. It will substantially prolong the talks (unless of course that is exactly what Russia actually wants). We need to make use of the experience of the INF talks, and the experience gained during the removal of Russian NSNW from the Warsaw Pact countries and the former Soviet republics. Clearly, France and Britain's participation is necessary in any consultations/talks on NSNW in Europe—but to begin with they should be observers rather than full participants. During the early stages at least, participation of third countries would only complicate the talks.

Another useful thing we could do is to formalize the existing presidential initiatives of 1991–1992 as a legally binding treaty—ideally with a verification mechanism. Such proposals have already been voiced by experts. There is no denying that because these initiatives are not legally binding, countries make their policy plans based on the worst-case scenarios. We could formalize the texts of these unilateral statements in a legally binding way. We could exchange information about the figures achieved following the implementation of the presidential initiatives. The United States and Russia could make a joint statement reaffirming their continued commitment to the unilateral statements made in 1991–1992. The NATO-Russia Council could once again become an important platform for exchange, the way it was back in the 1990s.

One more necessary step is negotiations on banning the deployment of NSNW in third countries, with a simultaneous removal of American NSNW from Europe back to the United States, with a complete and irreversible dismantlement of the entire NSNW infrastructure in Europe. But Europe cannot be turned into some kind of NSNW-free zone—not only because of the French factor, but also because various Russian NSNW delivery systems all have a different range, and some of them can reach NATO territory even if they are deployed east of the Urals. In addition, redeployment of Russian NSNW to bases east of the Urals—which is what the United States and some NATO countries are calling for—would complicate relations between Russia and China, Russia and Japan, and the United States and Japan. It could also meet with a negative reaction among the Russian public because questions of storage conditions and of the location of the depots, and questions of NSNW numbers, which are currently being kept off the agenda, will become a subject of more or less public debate in Russia.

TRANSPARENCY IN U.S.–RUSSIAN NSNW TALKS

BUZHINSKY: At this stage the only realistic step on NSNW is to agree some confidence-building measures. That will require progress in resolving the existing differences in the area of arms



control, including missile defense, non-nuclear strategic offensive weapons, and the non-placement of weapons in space.

There is a set of confidence-building measures which Russia and the West could agree in order to increase transparency with regard to NSNW: greater transparency, “separation” of ammunition and delivery systems, ensuring the security of nuclear ammunition, and commitment not to increase stockpiles.

Greater transparency. Russia and the United States have sufficiently accurate information about the location of the depots where non-strategic nuclear ammunition is being stored—but the information about their numbers is far less accurate. As a first significant step, Russia and the United States could release official figures about the size of their NSNW stockpiles and the numbers of tactical nuclear weapons currently awaiting their turn to be dismantled.

“Separation” of ammunition and delivery systems. All Russian non-strategic nuclear warheads are being stored separately from the delivery systems. By way of another confidence-building measure, the two sides could agree the text of official statements saying that nuclear munitions are being stored separately from the delivery systems, and that neither Russia nor the United States has any plans to change the situation.

Ensuring the security of nuclear ammunition. Based on their joint experience as part of the mutual threat reduction program and the NATO-Russia Council, Russia and the United States could undertake the following measures:

- assess the risks of terrorists gaining access to nuclear ammunition storage depots and stealing nuclear weapons;
- assess measures to improve the security and safety of nuclear ammunition storage depots;
- conduct joint training events aimed at preventing theft of nuclear ammunition and fissile materials.

Commitment not to increase stockpiles. As a first step towards limiting NSNW stockpiles, Russia and the United States could declare a commitment not to increase those stockpiles.

The new NATO Strategic Concept contains a proposal that Russia should move its NSNW to storage depots far away from its western borders with the NATO countries. Obviously, such a proposal would be too costly to implement. Besides, it does not make much operational sense for Russia because such a step would significantly weaken the capabilities of the Russian Armed Forces—and especially of the Russian Navy’s Northern Fleet.

The NSNW confidence-building measures I have outlined would facilitate progress on a broader range of political and security issues.

There is also another sensitive problem which will have to be resolved if the United States and Russia agree to undertake confidence-building steps. There is no doubt that Russian transparency with regard to NSNW is important to the European countries. But Russia would hardly welcome Washington’s intention to share information about the Russian NSNW stockpiles with its NATO allies. One possible solution would be to make France, Britain, and the NATO nuclear capability part of the confidence-building process.

DYAKOV: The United States and NATO realize that negotiations are hardly possible. The only realistic possibility is unilateral steps aimed at increasing transparency. At least two key steps need to be made.

First, Russia and the United States should release official figures about the numbers of NSNW that have been eliminated. I would like to ask my fellow experts: would such a step really do any damage to our security? I invite people from the MoD to convince me that such a move would undermine our security. I am ready to listen to their arguments.

Second, we could end all speculation in the West about Russia allegedly having deployed its NSNW close to its western borders. In actual fact, both we and the Americans know very well where those weapons are being kept. Which is why, as a first step, we could take inspectors to the forward bases where those weapons used to be kept, and show them that there is nothing there anymore. That could be the first step—and then we shall see what we shall see.

And the last thing I would like to say today: at some point in the future, sooner or later, both sides will begin verifiable reductions of strategic as well as tactical munitions, and they will need verification measures. That is why Russia and the United States could continue the work on developing transparency measures which was undertaken in the 1990s.

BUZHINSKY: I would like to add that the United States is also concerned with making sure that nuclear stockpiles are not ramped up. U.S. profound expert Steven Pifer's idea about a single ceiling has gained a lot of traction. The essence of the idea is that the sides should agree an overall limit of 1,500 or 2,000 nuclear weapons, and then decide for themselves how to distribute that allowance between their strategic and tactical weapons. They can choose to have 100 strategic and 1,400 non-strategic weapons, or vice versa. But this idea is made impractical by the U.S. concept of operationally deployed warheads and by the concept of a strategic balance.

Senator Sam Nunn has proposed a way of overcoming this impasse; the idea is essentially to move along four separate tracks. I was in Munich when that report was being discussed. It found no support among the Russian participants. It is good as a slogan.

EVGENY ILYIN (RUSSIAN MINISTRY OF DEFENSE): The NSNW problem is very complex, but it is an attractive subject for discussions and assessments.

In our assessment, NSNW are not a destabilizing factor at this moment. First, their readiness status is a lot lower compared with strategic nuclear weapons. All non-strategic nuclear weapons are being kept at storage depots, and the risk of their unauthorized use is essentially zero. Second, the Russian Military Doctrine clearly describes the situations in which the use of NSNW can be authorized by the president.

As for the need for consultations, talks, or voluntary transparency measures concerning nuclear weapons, I would like to say that there has been an interesting discussion as to who needs this more—ourselves or the Americans? What is the MoD's opinion about the effects of NSNW reductions or limitations on our country's defense capability? The political goal of achieving a nuclear zero has been declared, and no one denies that. But what practical contribution can be made to increasing our defense capability or reducing the likelihood of conflicts in Europe by imposing limitations on NSNW, or by greater transparency? It would be useful for us in the MoD to hear some arguments in that regard.

I have heard several specific proposals today, which could be useful as voluntary or negotiated transparency measures, and which could be introduced in the near future. I am talking primarily about separating warheads from delivery systems—but in fact that measure has already been introduced; warheads and delivery systems are already being stored separately. The second issue is improving safety and security at the storage facilities. The official position of the Russian leadership is that adequate safety and security measures are already being provided using our own resources. According to the chief of the Russian General Staff, who was speaking at a NATO-Russia Council meeting, we are providing adequate safety and security measures for nuclear weapons; we are entirely capable of providing those measures on our own, now and in the future. Another proposal is to exchange information about the numbers of weapons that have already been dismantled. As far as demonstrating that the two sides are ready for dialogue is concerned, such a step is entirely possible. But in my view, as an expert, that step would not have any practical implications. On the whole, I believe that releasing the official numbers has become something of an obsession. So let's say we have this figure—what does it matter if it changes by 100 weapons in this or another direction?

Any arms reduction process must pursue three goals: reducing the likelihood of a conflict; making the Armed Forces cheaper to maintain; and improving the sense of shared security. As far as shared security is concerned, making declarations and releasing figures may well help that process. But the first two goals, which I think are the most important, will not be served in any way by declaring the numerical indicators. From the MoD's point of view, our objective is to increase our country's defense capability, not to reduce it; at the very least, we should not do anything to harm it.

Finally, let me say a few words about confidence-building measures. In my view, these measures must be specific, and they must have a clear goal. At this moment, having listened to the experts' opinions, I can say that the discussion has been useful. We have discussed the things that can be done in the immediate future, the things we can expect. But we must set more specific goals. There must be a clear understanding of how all the proposed measures will help to augment the



Russian defense capability, among other things. I'm afraid I must disagree with the colleague who said that whether we want it or not, we will have to take these steps. I don't think that is the case. These steps will require both sides' agreement.


If we want it, it will be a bilateral process. But we must see positive outcomes for Russia.

RYBACHENKOV: I am finding it difficult to understand the position of the MoD representatives. They seem to argue that the NSNW problem simply does not exist. But we do need progress on NSNW (information exchange)—if only to keep the process going. Otherwise, how are we going to demonstrate progress in implementing Article VI of the NPT at the 2015 Review Conference?

ILYIN: I am voicing my position as an expert who is currently serving with the MoD. The MoD is responsible for our national security and defense capability. That is why I have asked the following question: "How will the measures you propose—including information exchange and increasing transparency with regard to storage locations—improve our country's defense capability?" As for the need to report at the conference and to come prepared—yes, I agree, we need to come prepared. We have the implementation of the New START treaty to report to the conference. Some people say it is not enough, others believe that it is. If we fully implement the commitments undertaken as part of the New START treaty, it will be a good demonstration of Russia's commitment to the terms of the NPT.

ORLOV: Obviously, there are different opinions in our expert community about the issue on the table, which is very sensitive from the Russian security point of view. There are official Russian approaches, which have been outlined today—and these are not just approaches preferred by some ministries and agencies; they have been approved by the top Russian political leadership.

Speaking at the meeting in Sarov on February 24, 2012, in answer to a question and a commentary by Evgeny Buzhinsky—who is present here today—Vladimir Putin has this to say about NSNW: "We are absolutely not going to relinquish any of the things that we actually need. We are going to relinquish only those things which have become a burden and are no longer of any use to us—it's as simple as that. The things which do not burden us, and which, on the contrary, provide certain security guarantees—we have no intention at all of relinquishing them." That, in fact, is the program for the next few years.

I believe that the proposals voiced by Evgeny Buzhinsky deserve to be looked at very carefully. In particular, I am talking about the idea of choosing the path of greater transparency without doing any damage to our national security—I think these proposals are well worth studying and discussing. Would it cause us any great harm to release the figures? I am not at all sure that it would. It may well be that after releasing those figures on a confidential basis we could do it publicly as well. We must do it based on our own interests, in a deliberate, step-by-step fashion. The practical question is, why not say how many weapons have already been destroyed? I think such a move would facilitate dialogue with our partners in the shared European security space. 

For more analytics on disarmament, please, visit the section "Ways towards Nuclear Disarmament" of the PIR Center website: disarmament.eng.pircenter.org

NOTE

¹ The text of this article is based on the materials from the workshop "The Future of NSNW in Europe: Problems and Solutions," which was hosted by the PIR Center as part of its project "Ways towards Nuclear Disarmament." We would like to thank the Foreign Ministry of Finland for its kind support in organizing the event.



Alexander Kmentt

NUCLEAR DETERRENCE AS A BELIEF SYSTEM

How does the current situation in the disarmament and nonproliferation area present itself from a non-nuclear weapon state (NNWS) perspective and address the visible disconnect that we see in the discourse on these issues? While these are some of my personal reflections I have been dealing with these issues for quite some time and I am confident that they may be along the lines of what quite a few NNWS are thinking. When I am talking about nuclear-weapon states (NWS), I will focus primarily on Russia and the United States and not address the other NWS or nuclear armed states.

Despite a successful 2010 Review Conference and despite the reductions in nuclear weapons (NWs) numbers between Russia and the United States, such as through the recent New START, it is disappointing for NNWS to see how little movement has been made since the end of the Cold War to change the approach to NWs in any fundamental way. NWs and the deterrence logic are today seen by many as a high-risk and high-stake poker game that humanity was incredibly lucky to escape from unharmed in the period of ideological competition between two hostile blocks during the Cold War. It is difficult to accept that the concepts of deterrence, mutually assured destruction, and the logic of nuclear strategic stability have simply been transferred into the twenty-first century and that the chance to remove this sword of Damocles from above our heads is not being seized with far more urgency.

During the Cold War, the nuclear stand-off may have been seen and accepted by NNWS as inevitable. But how is it that essentially the same nuclear standoff is still in place and, despite reductions in numbers, thousands of warheads are still on hair-trigger alert, and that big population centers are still being targeted? Considering and understanding the practical difficulties related to a nuclear disarmament process, it is deeply disappointing that NMs have not been fundamentally reassessed, that their use has not been clearly taken out of nuclear doctrines, and that no agreement has been reached to put NWs in storage out of operational deployment and off high alert. Russia and the United States appear to continue to feed on each other's threat and enemy perceptions to justify the possession of NWs and the maintenance of a large NWs infrastructure, even though the ideological confrontation is gone. It is striking how the NWs logic is continued even though the prime justification for the Cold War nuclear confrontation has disappeared.

The existence of NWs is no longer justified by the (perceived) need to deter an attack by a mortal ideological opponent. Nuclear deterrence looks today as if it has become an end in itself. There is no longer the need to deter against someone but simply the need for deterrence as such. There is thus a deeply disconcerting perception among NNWS that the United States and Russia (followed by the other NWS) are trapped in a highly dangerous Cold War thought-system which renders them incapable of addressing and solving the NWs issue in a fundamental way, let alone giving up NWs.

Some refer to deterrence as a "belief system." And I think this is very true. No one actually wants NWs to be used or conceives that they will be, but the belief in their value as the ultimate guarantee of security persists. NWS have been unable and/or unwilling to challenge this belief system.



The logic of nuclear deterrence is posited and of course still argued coherently. Strategic stability, strike, and counter-strike capabilities etc. are all logical and compelling, yet it is a fundamentally absurd belief system. It is absurd because of the high stakes and the unacceptable humanitarian effects that one failure of the belief system—accidental and deliberate—would cause. It is absurd to trust that nuclear deterrence will remain stable and provide security in the long run with an increasing number of nuclear armed actors. The reasoning that governments are rational enough to handle nuclear deterrence and that nuclear deterrence works because it makes governments act rationally is essentially the most dangerous circular argument in human history.

I believe that NWS have largely failed to provide convincing arguments to state against whom deterrence, from their point of view, is necessary today and justified. In the case of Russia, we see the continued drive for nuclear parity with the United States. But, with ideology gone, what is the reason for this and what is the real underlying threat perception? What is the role that Russia sees for itself in the world of today that requires this nuclear parity? The same question must go to the United States as well as the other NWS. Where is the threat today that justifies NWS as a response other than the existence of nuclear arsenals in other states that are maintained because of a similar deterrence belief?

While nuclear deterrence arguments may be given as the main reasons for the retention of NWS, this is, however, only part of the story. There is a strong psychological element associated with NWS. The power status of states possessing NWS, the status quo of the post-World War II world order, former status as global powers, such as in the case of the UK and France, and perceived admission to global power status, such as for instance in the case of India, these are all aspects that have been linked to the possession of NWS. In my opinion, this is a tragic misjudgment by NWS: that they have not used the moment of the end of the Cold War to diminish the role and status of NWS. This neglect is one of if not the key driver for the proliferation of NWS. If we then hear, as we have a few times in the NPT Preparatory Committee, arguments from NWS that cite the existence of proliferation as reason to retain NWS, we are faced with another circular argument that is used to remain firmly in the belief system that justifies the retention of NWS.

NWS may have in theory embraced the long-term aim of a world without NWS, such as the United States through President Obama's Prague speech and in the outcome of the 2010 NPT Review Conference. However, there are some serious question marks—to say the least—in the minds of an increasing number of NNWS as to the sincerity of NWS for real nuclear disarmament rather than a readiness to commit to limited arms reduction and control measures.

I would therefore say that there is a serious disconnect between the lines of argumentation of NWS and the way many if not most NNWS look on the issue. NWS have come to symbolize a system that is deeply unfair and the reasons given for the continued retention or for unwillingness to fundamentally address the approach to NWS are seen as either irresponsible or anachronistic or both.

Given the devastating consequences of NWS, most NNWS today see it as unacceptable that such an existential threat to all humankind continues to be handled by a few states as a national security matter. The notion that it is the right and legitimate interest of all states to be actively engaged in global security matters and nuclear disarmament is not just an empty phrase. I firmly believe that this is a consequence of globalization and an understanding of interconnectedness, which will only increase further.


What we see instead are flawed multilateral processes that are dominated by obvious tactics to maintain the status quo for as long as possible. The NPT is maybe the best but not the only example of this. The consequence of all this is an increasing erosion of legitimacy of existing legal frameworks.

I would therefore argue that NWS should take much more seriously the views, concerns, and expectations of NNWS that I have tried to outline. The tactics of playing for time within the NPT and the other multilateral fora may not work for much longer. I would argue that this NPT review cycle is of crucial importance. It will largely determine to what extent the NPT is a credible framework for nuclear disarmament. And there is also a race against time. The global regime can either be maintained and maybe even strengthened and the spread of NWS stopped. Or the legitimacy of the NPT and the entire regime will be so undermined with the potential consequence of more and more actors seeking to develop NWS. NWS have the prime responsibility to prevent this but they need to realize with urgency that in the final consequence they cannot have it both ways.

So I propose this “idea” for Russia, which is to become a leader on this issue and live up to its disarmament commitments in a credible way and implement the 2000 13 disarmament steps and the 2010 action plan. In addition, I hope Russia would enter into open and transparent discourse on the NWS issue in a broad sense, including the validity of nuclear deterrence in the twenty-first century, threat perceptions that exist today justifying nuclear deterrence, the proliferation risk that this behavior generates and all of this measured against the risk of inflicting unacceptable harm and unspeakable humanitarian consequences to all humankind.

For more information and analytics, please, visit the section “Nonproliferation and Russia” of the PIR Center website: npt.eng.pircenter.org

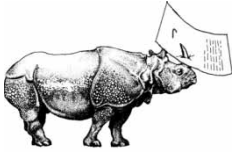
Now, I know that most Russian arms control experts would smile and basically say: “nuclear disarmament, yes, nice but get real.” I would counter this by saying that the military security approach towards NWS that appears to be so dominant in Russian discourse today is not cast in stone in Russia or in any of the other NWS. Civil society will also play an increasing role in Russia, some elements of which we are already seeing today. Pressure for greater transparency and scrutiny of governmental action and priorities will also increase in Russia, coupled with an unstoppable trend for more global interaction and global empathy.

So ultimately, I am optimistic that the discourse on NWS will change in Russia as well as in the other NWS. Instead of resisting and acting counter to the clearly expressed global aspirations, I hope that elites in NWS will increasingly embrace this thinking themselves. 

NOTE

* This article has been prepared on the basis of a statement by Ambassador Alexander Kmentt at the seminar “Nuclear Nonproliferation and Disarmament: Ideas from Russia, Ideas for Russia,” held by the PIR Center and the Vienna Center for Disarmament and Non-Proliferation on May 8, 2012.





Andrey Baklitsky, Evgeny Buzhinsky, Pavel Luzin, and Oleg Demidov

HIGH TECH ON BRICS AGENDA: WHAT COULD RUSSIA PROPOSE?

Economic growth and the combined demographic, scientific, and industrial potential of the BRICS countries have turned the bloc into a global leader. Other global players are paying close attention to this format of international cooperation. BRICS nations are already working closely in the area of finance, but there is clear room for improvement in terms of cooperation in high-tech industries, which are crucially important for international security and economic growth.

Cooperation in the high-tech sector between the BRICS countries could go a long way towards resolving several global problems. In addition, it could further institutionalize the BRICS structure and give it greater practical meaning. Russia has traditionally been a leader in high tech. Using Russian experience in the BRICS format could therefore enable our country to play a more active role in addressing these problems and bolster its own standing in that informal bloc.

The most promising areas of cooperation in the high-tech sector include:

- countering cyberthreats;
- safe and secure development of nuclear energy;
- peaceful space exploration;
- high-tech technologies in the logistics sector, such as radio-frequency identification (RFID) technology.

One of the key modern trends is the rapid development and spread of new technologies. Over the coming decade that trend will become even stronger. Advanced technologies are often put to military applications. In many areas, the United States and its allies—the European countries, Japan, and South Korea—have come to dominate this technological race. The uneven and uncontrolled nature of growth in the above-mentioned areas is detrimental to the existing balance in the international system; it could even provoke a new arms race.

Russia remains one of the world's most technologically advanced countries. But rapid technological progress in the developed countries and the significant efforts being made by the developing nations to close the gap with the leaders are jeopardizing Russia's standing. Lagging behind the world leaders in peaceful technologies means a loss of international competitiveness.

INTERNET TECHNOLOGIES

It has become obvious in recent years that the BRICS nations must radically step up their cooperation in fighting cyberthreats. There is a clear deficit of effective mechanisms against transnational cybercrime. Meanwhile, criminals are developing ever more sophisticated and destructive types of cyber-weapons. As a result, the critical infrastructure of countries around the world is becoming extremely vulnerable to such threats. While the people who perpetrate cyberattacks and the ones who pay for them remain anonymous, the attacks themselves are



becoming increasingly destructive, and the damage they inflict is not limited to the cyberworld. Such a situation inevitably undermines the existing international security regime and destabilizes the international system. That is a direct threat to the national security of Russia and its allies.

Other problems include variations in the development of internet infrastructure across the globe, which could slow down further progress and rollout of Internet technologies in the developing countries.

Using the BRICS format, Russia could initiate the development of a strategy document summarizing the shared vision and outlining the consensus approach of the BRICS nations to the provision of security for the information space, as well as stating the goal of promoting such an approach at various international platforms, including the UN and its specialized agencies. The BRICS nations need to draw up a series of agreements to ban cyberattacks against critical infrastructure of the financial system, nuclear energy facilities, and strategic military command systems, as well as information systems of offensive weapons and WMD.

BRICS could become a format for confidence-building measures and information exchange in the area of cybersecurity between the participating states. Such measures could include development of systems to prevent cyber-incidents, provide early warning, and share information about them. In particular, the BRICS nations could establish emergency hotlines and an international center for dealing with cyberthreats, using mechanisms of international public-private partnership.

It would be in the interests of BRICS as a whole and of Russia in particular to pursue joint projects which aim to improve the intercontinental IT infrastructure (fiber-optic cables, etc). Such projects would increase the reliability and resilience of telecommunication channels between the BRICS countries, and give people living in these countries greater access to broadband Internet. One possible project—which is already being discussed—is to lay a transcontinental underwater data cable directly connecting all the BRICS countries, which are situated on three continents.

All five BRICS nations have more or less equal starting positions, shared problems, and similar obstacles to active and rapid development of e-governance and, in a broader sense, of information society as a whole. Setting up a coordinating structure to facilitate the sharing of best international practice and to assist in the adoption of that practice would help to achieve the common goals.

PEACEFUL SPACE EXPLORATION

The dangerous possibility of weapons being placed in outer space still remains on the international security agenda. International space law has many gaps in terms of regulating the use by sovereign states of outer space, and near-earth space in particular. It allows the placement and deployment in space of non-nuclear weapons, as well as the use of force in space and from space. In February 2008 Russia and China jointly unveiled a draft treaty which aims to prevent the placement of weapons in space, as well as the use or threat of the use of force against spacecraft. But the draft, which was proposed for the consideration of the Conference on Disarmament in Geneva, has not received the required international support. Even though by now many countries have reacted positively to the Russian-Chinese initiative, Brazil and India, which have their own military space programs, have been less than enthusiastic. In addition, there is little coordination between the BRICS countries at the Conference on Disarmament—or any other forums, for that matter—on the issue of using space for peaceful purposes.

At the same time, the benefits of actively developing peaceful space technologies are being partially devalued by R&D duplication (for example, the global satellite navigation systems and independent space programs pursued by individual countries). As a result, resources are not being concentrated on the important task of radically improving satellite navigation technologies or exploring interplanetary space. The Russian space industry is also facing several difficulties stemming from the inadequate presence of Roskosmos in the southern hemisphere (there is a need for additional correction and monitoring stations for GLONASS, and for more orbit observation instruments).

Russia must lobby all fellow BRICS members to secure their support for the initiative on banning the placement of weapons in outer space. First and foremost, efforts must be made to persuade India and Brazil to change their stance. These two countries' concerns in this area need to be

clearly understood, and then addressed and eliminated. Once that has been achieved, the BRICS countries will be able to form a united front at the Conference on Disarmament, at the UN Committee on the Peaceful Uses of Outer Space, and during formal and informal consultations with the United States and other nations.

It would be in Russian interests to sign an agreement on using the territory of South Africa, Brazil, and India for joint orbit monitoring, tracking exploration spacecraft in deep space, and extending the coverage and improving the accuracy of the GLONASS system. Russia needs to promote GLONASS in the BRICS countries; the Russian satellite navigation system should be used in conjunction with the existing and future systems operated by India and China.

Joint space initiatives of the BRICS nations should aim to create an attractive global alternative to the U.S. and EU space programs.

NUCLEAR ENERGY

Even though it has been more than a year since the Fukushima nuclear accident, the issue of safety and security of nuclear power plants and of the entire nuclear industry remains as pressing as ever, with major repercussions for that industry's prospects. At the BRICS summit in Delhi on March 30, 2012 the leaders of the five countries called for international cooperation in the development of safe and secure nuclear energy. The BRICS heads of state highlighted the need for joint efforts in order to "increase public trust in nuclear energy as a clean, affordable, safe and reliable source of energy, which is indispensable for meeting the world's energy demand."¹

In the context of developing nuclear technologies in the BRICS countries, the most sensible approach for Russia would be to transition from building power plants in these countries to partnership and joint projects, primarily with India and China. Russia should seek to engage companies from these two countries (and, at some point in the future, from Brazil and South Africa as well) in consortiums to build NPPs in the BRICS countries themselves and in third countries. Such projects would strengthen ties between the five BRICS nations through partnership relations between their companies. They would also enable greater use of the credit resources of the BRICS states in third-country NPP projects. Participation of national companies in these projects would help to build trust among the local population and to avoid protests. In return, Russia will be able to secure preferential access to the markets of its partners.

Russia needs to participate in joint nuclear research projects with the other BRICS countries in order to strengthen its ties with its partners and to reduce the influence of third countries, as well as to improve its own nuclear energy technologies. New technologies developed by the BRICS nations (based, for example, on thorium cycle research by China and India) could bring substantial changes to the global energy sector.

The BRICS countries also need to develop nuclear energy cooperation between their scientists and expert communities. Contacts between experts and specialists, as well as academic exchange programs, can help these countries to build up their own expertise, demonstrate to the decision-makers the benefits of cooperation with Russia, and establish the necessary ties.

HIGH TECHNOLOGIES IN LOGISTICS

The BRICS countries are the world's leading economies—but trade between them is well below its full potential. In 2011 mutual trade in the BRICS bloc stood at \$230 billion. The BRICS summit in Delhi held in March 2012 has set the target of \$500 billion, to be achieved by 2015. The five countries urgently need to optimize their cross-border logistics and speed up the transit of goods, while at the same time improving the reliability of customs controls. There are high-tech solutions available, such as radio-frequency identification (RFID) technology, which relies on radio waves to transmit information, either manually or automatically. They could help to improve the situation. But the BRICS countries are not putting these technologies to good use, and their efforts in this area lack coordination. In addition, there is no single set of RFID standards, and only a relatively small number of checkpoints are equipped with that technology.

Like all the other BRICS countries, Russia has a clear interest in optimizing the flow of trading goods and introducing automatic identification of cargos. BRICS nations could jointly develop a common standard of radiofrequency identification to speed up the work of the border and



customs checkpoints in the five countries. Such a standard could also be adopted on a global scale. It would also make sense for all BRICS countries to study the Indian initiative on equipping all the national checkpoints with RFID technology.


RUSSIA'S INTERESTS

Russian interests in high tech boil down to neutralizing the military threat in space and peaceful space exploration; developing Internet technologies and countering threats in cyberspace; preventing a new arms race; maximizing the Russian potential in nuclear energy; and introducing advanced technologies in the logistics industry. High-tech branches of the Russian economy also require foreign investment and innovation.

It is also important for Russia to strengthen BRICS and to flesh it out with various forms of political, economic, and technological cooperation.

The combined potential of the BRICS countries is very impressive;² this also applies to the high-tech sector. However, making use of that potential is difficult because of the lack of a common agenda and action plan in the area of high technologies. Cooperation is mostly happening on a bilateral rather than multilateral level.

Making use of the opportunities offered by BRICS to compete more successfully with the United States, the European Union, Japan, and other developed economies is in the interests of Russia and all the other BRICS nations. To that end, Brazil, Russia, India, China, and South Africa must turn from a financial club into a group of countries united by the scope of their shared interests, and willing to defend these interests in the international arena. Russia's place in this body should be appropriate to its level of technological development.

Russia's interests require a shift in the focus of cooperation within the BRICS bloc towards areas which constitute our country's traditional strengths. Such a shift will be made easier by the fact that our BRICS partners are genuinely interested in the development of high-tech sectors. By the same token, it is clearly in Russia's interests to strengthen its economic presence in India and China, and to expand it geographically by stepping up cooperation with Brazil and South Africa. 

NOTES

¹ Delhi Declaration, President of Russia—official website, March 29, 2012, <http://eng.news.kremlin.ru/ref_notes/82>, last accessed January 15, 2013.

² BRICS countries account for about 70 percent of the world's nuclear power plants now under construction. Russia, China, and India accounted for 62 percent of the world's space launches in the first half of 2012. The Russian segment of the Internet is the largest in Europe, and China's the largest in the world. All five of the BRICS national segments are among the fastest-growing in the world. Half of the world's Internet users live in BRICS countries.



Maksim Simonenko

STUXNET AND NUCLEAR ENRICHMENT OF THE CYBER SECURITY REGIME

Experts and decision-makers in countries all over the world have recently been pondering the interrelationship between nuclear and information technologies—especially in the context of security challenges and threats that have suddenly emerged at this technology crossroads. The issue became especially poignant in the summer of 2010 following the emergence of the Stuxnet virus, which apparently targeted the Iranian nuclear infrastructure. Experts and media commentators speculate that the malware was written specifically to disrupt industrial control systems (ICS) at Iran’s Bushehr nuclear power plant and the enrichment facility in Natanz.

But industrial control systems of that type are commonly used at many other industrial facilities all over the world, from power grids and uranium enrichment plants to Chinese soft toy factories. The underlying technology is much the same, regardless of what the facility in question does. The expert community and the political decision-makers are therefore faced with the question of whether it actually makes much sense to focus only on the information security of nuclear facilities as opposed to industry as a whole. The answer to that question will shape the national and international strategies for providing information security of nuclear infrastructure. So far, the international agenda in this area seems extremely vague; there is no sign of a common international approach to the problem.

On the other hand, IT experts are confident that some of the experience accumulated in the nuclear age is relevant to building a universal international regime of information security. Such views have become even more prevalent since the discovery of the Stuxnet virus. It is no coincidence that in the summer of 2012 the head of the Kaspersky Laboratory, Evgeny Kaspersky, voiced the idea of establishing a cyber-IAEA, i.e. an international mechanism which replicates the IAEA approaches in the area of information technologies. The purpose of such a mechanism is to lay the foundations of an international information security regime based on a system of monitoring and mutual commitments, with the ultimate goal of preventing a cyber arms race and cyber wars.

The idea appears plausible—but it does raise a number of questions. How relevant are the methods and strategic axioms of the nuclear deterrence theory when applied to cyberspace? If we want to be safe from things like Stuxnet, would it be enough for all countries to develop a common code of conduct in cyberspace, and declare it a zone free of cyberweapons? Is such cooperation between states feasible—even if we forget for a minute that we also need to take the non-state actors into account? Speaking metaphorically, at this point the edifice of the international information security regime not only lacks a foundation; in fact, even the blueprint of that edifice has yet to be drawn up and approved. Meanwhile, there is no time left for procrastination.

For more analytics on information security, please, visit the section “International Information Security and Global Internet Governance” of the PIR Center website: net.eng.pircenter.org

New versions of complex malware similar to Stuxnet—such as Flame, Duqu, and Gauss—are being detected once every few months. Nobody can predict what devastating blow the next sophisticated cyberweapon will inflict, or when. Such questions are forcing us to take a much



closer look at the now-infamous virus which attacked the Iranian nuclear facilities, and try to find some important answers. Who wrote Stuxnet? What for? Has it performed as its authors expected? We need these answers to understand what kind of regime we need to build in order to counter such threats; who we can build it with; and when. We need to know what exactly such a regime should look like, and what elements it can borrow from the doctrines of the nuclear weapons age.

ANTI-NUCLEAR CYBER-WEAPONS?

In June 2010 VirusBlockada,¹ a Belarusian computer security company, was the first to detect RootTmPhider, a sophisticated virus which later became known as Stuxnet. The malware was targeted against automated control systems used at industrial facilities. By year's end the virus had infected about 100,000 computers in different countries. Most of those computers were in Iran (58.3 percent), Indonesia (17.8 percent) and India (10 percent).² But the epidemic was already well under way when the virus was first detected, so there is no reason to believe that the countries with the greatest numbers of infected computers were the same countries where the malware had originated.³ That conclusion is borne out by official statistics released by Siemens, the maker of the industrial control system targeted by the virus. According to an official statement released by the company, in March 2011 there were 24 known cases of its clients' industrial control systems being infected.⁴

Stuxnet is undoubtedly a very sophisticated piece of malware, a product of a large and highly competent team of developers. It has often been mentioned that the virus uses as many as four previously unknown zero-day vulnerabilities. It also relies on several stolen security certificates from large component manufacturers in order to disguise its nature. Finally, its makers seem to have had access to formidable expertise in the area of industrial control systems. All of these pieces of evidence have led experts and media commentators to conclude that Stuxnet was developed by a state or a group of states. The virus has often been described as an extremely sophisticated weapon used by that state or group of states to further their national interests.

If we accept that argument, we have to recognize that Stuxnet is a cyberweapon of colossal destructive power; in theory, it could be as destructive as WMD. In mid-June 2012 Kenneth Benedict, executive director and publisher of the *Bulletin of the Atomic Sciences*, compared the impact of the virus to the nuclear bombings of Hiroshima and Nagasaki.⁵ When experts discuss threats originating in cyberspace, they often use concepts that date back to the Cold War era—namely, the concepts of deterrence and retaliatory strike. Such an approach has even been incorporated in the Pentagon's official cyber strategy, which equates cyberattacks to conventional military attacks, and says that all available weapons—including nuclear—could be used in retaliation.⁶ The already mentioned cyber-IAEA proposal by the head of the Kaspersky Laboratories is aimed specifically at preventing the militarization of cyberspace and a cyber arms race. The Russian expert believes that merely establishing some mechanism for cyber arms control would not be enough; he argues that such a mechanism "should copy the international nuclear security system and replicate it in cyberspace."⁷

Talking about cyberweapons, it is important to establish who or what their targets are. At present there are two completely opposite views about the objectives pursued by the developers of Stuxnet. The first emerged after the source code of the virus became available on the Internet⁸ in August 2010, enabling a broad international community of information security experts to study that virus. By mid-September Ralph Langner, a German cybersecurity expert, voiced the theory that Stuxnet developers were aiming for a specific target.⁹ Shortly afterwards that target was identified; it turned out to be an information exchange system between the SIMATIC S7 programmable logic controller and the SIMATIC WinCC industrial workstations, both made by Siemens. Experts then began to speculate that the virus may have specifically targeted industrial control systems of the Bushehr nuclear power plant in Iran. That is when non-specialist media started to mention Stuxnet in the context of the Iranian nuclear program.¹⁰

After the media obtained the information about the virus, Mahmoud Jafari, a project manager at the Bushehr NPP, said that Stuxnet had infected only personal workstations of the NPP's personnel.¹¹ But Mahmoud Liayi, secretary of the Information Technology Council of the Industries Ministry, then went on the record as saying that "the Stuxnet spy worm has been created in line with the West's electronic warfare against Iran."¹² As a matter of fact, none of the officials had recognized that the virus specifically targeted the nuclear power plant's industrial

control systems; Liayi even claimed that Stuxnet was merely a piece of spyware. But in early 2011 Dmitry Rogozin, the Russian envoy to NATO at the time, urged the alliance to conduct a thorough investigation of the Stuxnet situation in order to prevent “another Chernobyl.”¹³

It was only much later, once the Stuxnet source code had been studied in much greater detail, that experts came up with another theory about the intended target. It turned out that the virus may have been written in order to damage enrichment centrifuges at the Iranian uranium enrichment plant in Natanz.¹⁴ In November 2010 analysts working for Symantec, one of the world’s leading cybersecurity companies, found that the worm targeted not only a specific industrial control system, but also a specific model of high-frequency inverters made Iran’s Fararo Paya and Finland’s Vacon,¹⁵ which has a manufacturing base in China.¹⁶

Experts from the Institute of Science and International Security (ISIS) speculated that inverters of that type may have been used at the uranium enrichment facility in Natanz.¹⁷ According to an ISIS report, in late 2008–early 2009 the Natanz facility’s output of low-enriched uranium suddenly fell for no apparent reason. The main version proposed by the Institute was that the Iranians had made some engineering errors during a project to increase the facility’s production capacity. During the period from May 2008 to November 2009 the number of operational centrifuges at Natanz went up from 3,280 to 4,920—but then went down again by 984 to 3,936.¹⁸ ISIS experts theorized that the 984 centrifuges may have been damaged by Stuxnet.

By late November 2010 Iranian President Mahmoud Ahmadinejad confirmed that “they [i.e. unnamed actors working at the behest of the West] succeeded in creating problems for a limited number of our centrifuges with the software they had installed in electronic parts.”¹⁹ But he said nothing about Natanz and did not specifically mention any virus. Then in February 2011 ISIS experts, having studied updated information about Stuxnet, withdrew their previous version that the virus was the reason behind the fall in the number of operational centrifuges at Natanz. They said that the relevant code in the virus was not activated and therefore could not have launched an attack.²⁰ In June 2011 Langner went even further and said he doubted that the virus specifically targeted gas centrifuge control systems.²¹

That, however, did not put an end to the Natanz version. In June 2012 the *New York Times* reported that senior U.S. and Israeli officials had been involved in preparing a campaign of cyberattacks, codenamed Olympic Games, against enrichment centrifuges in Natanz.²² It said that Stuxnet was one of the instruments of those attacks. According to media sources, “within a week [of the virus being detected] another version of the virus disabled about a thousand centrifuges.” So far, this appears to be the only assertion that can potentially be verified using open-source information. But there is nothing to suggest that Iran had any problems with gas centrifuges in the autumn of 2010; on the contrary, its centrifuge enrichment program seems to be doing well. On February 15, 2012 the number of centrifuges in Natanz went up again by as much as 30 percent to 9,000 units.²³ By the end of the summer of 2012 the figure had topped 10,000. That seems to belie the idea that Stuxnet was developed to sabotage the centrifuges in Natanz—or perhaps the virus did in fact target the centrifuges, but the cyberattack failed.

In this situation the tried-and-tested way of identifying the attacker by identifying the target of the attack does not work because nothing is known for certain about which particular target the attackers had in mind. At the same time, claims of the virus being extremely sophisticated may be somewhat exaggerated. For example, some of the “previously unknown” zero-day vulnerabilities used by Stuxnet were actually known before the arrival of the virus. According to a Symantec virus database, the vulnerability in the.lnk files was used back in late 2008 by another virus. Information about the print spooler vulnerability had been published in *Hakin9*, a specialist cybersecurity journal, before it was used in Stuxnet.²⁴ This means that the team which wrote the virus had to find only two new vulnerabilities out of the four used in Stuxnet; the other two could have been acquired on the black market or found in specialist literature. The digital security certificates which were used to sign the virus could have been stolen from the two component manufacturers, Realtek Semiconductor Corp и JMicron Technology Corp, using standard techniques—especially since both companies have their offices in Hsinchu Science Park in Taiwan.²⁵ One possibility is that the certificates were stolen with the help of the Zeus trojan, which specializes in stealing bank details, but which could have been used to obtain the certificates as well.

As for the virus-writers’ expertise in the area of industrial control systems, one possible source is the U.S. National SCADA Test Bed Program (NTSB), which was undertaken in 2003–2009 to



assess the cyber security weaknesses of common industrial control systems. In the spring of 2010 the program released a final report which contained a detailed description of various possible threats.²⁶ One interesting connection to Stuxnet is the 2008 Siemens Automation Summit, which was held as part of that program. The summit included a report and a presentation by Marty Edwards of the Idaho National Laboratory and Todd Stauffer, who works at Siemens, focusing on possible vulnerabilities of the industrial control system which was later targeted by Stuxnet.²⁷ That information could have been used by the developers of the virus.

Based on all of the above we can assume that the actors behind Stuxnet are not necessarily states. By the same token, the virus should not necessarily be viewed as a digital Pearl Harbor or a digital Hiroshima. A single shot fired by an unknown perpetrator does not always signify the opening of hostilities; similarly, there is no reason to equate every single use of a cyberweapon to the launch of a cyberwar. “A cyberattack that shuts down the power grid might be part of a cyberwar campaign, but it also might be an act of cyberterrorism, cybercrime, or even...cybervandalism. Which it is will depend on the motivations of the attacker and the circumstances surrounding the attack...”²⁸

One of the most creative but least discussed studies of the possible targets and perpetrators of the Stuxnet attack is a paper by Jeffrey Carr, head of Taia Global, a cybersecurity firm. It was written specially for the 2010 Black Hat hackers' conference in Abu Dhabi. The main Stuxnet targeting scenarios proposed by Carr focus on the possibility that the virus was developed as an instrument of cyberattacks against rare-earth-metals-producing states or uranium-producing states; as an instrument of corporate sabotage to discredit Siemens; or as part of a Chinese strategy of protecting the Malacca Straits.²⁹

According to the first scenario, Stuxnet was an attempt by a commercial company to sabotage the competitors' mining operations in order to become the dominant global supplier of rare-earth metals. The uranium scenario suggests that the cyberattack was initiated by a rich environmental NGO known for its anti-nuclear stance (such as Greenpeace). According to the anti-Siemens scenario, France's Areva may have been interested in discrediting Siemens ahead of the signing of a joint venture deal between the German giant and Russia's Rosatom. Finally, the Malacca Straits scenario points out that China has a strategic interest in that waterway, which is crucial to Chinese national energy security and foreign trade.

To summarize, it is not just state actors but also commercial companies and NGOs who, in theory, had the motives and the capability to create a virus such as Stuxnet. Another important thing to consider is that, as this paper has already demonstrated, non-state actors (cybersecurity companies, NGOs, research centers, and even individual researchers) have also made a significant contribution to detecting, studying, and neutralizing Stuxnet. That is why, if we want to create an effective international cybersecurity regime, we must take into account the constructive as well as destructive impact of non-state actors on cyberspace.

LESSONS FOR THE INTERNATIONAL COMMUNITY

The arrival of Stuxnet has significantly accelerated the militarization of cyberspace. We are witnessing the process of institutionalization of various strategies for using cyberspace for military purposes. The defense ministries of the leading nations are setting up cyber teams which develop strategies for action in cyberspace. The scenarios of large military exercises are increasingly being amended to include warfare in cyberspace. Some are already voicing suspicions that military planners and the corporate world are deliberately hyping up the magnitude of the cybersecurity threats we are facing.³⁰ These suspicions are not entirely groundless—but what are the real lessons the world should learn from the emergence of such a sophisticated virus?

Martin Libicki, a senior analyst with RAND Corporation, says that cyberweapons have a specific set of distinguishing features.³¹ To begin with, they are capable of delivering surgical strikes, without disrupting other elements and systems of the IT infrastructure on which people have come to depend so much in so many areas, from motoring to high-precision weapons targeting systems. Second, cyberweapons are not really reusable. Once a vulnerability targeted by a specific piece of malware becomes known, it is quickly patched up by cybersecurity specialists. Third, it is very difficult to identify the people who commission the development of cyberweapons. Fourth, it is also very difficult to assess the power and the destructive potential of any individual

cyberweapon due to the lack of information about its intended targets, and also because the criteria for making such assessments are hard to formulate.

Of all the characteristics of cyberweapons, lack of reusability is probably the most relevant when talking about technological countermeasures. But here we have the precedent set by Flame, a computer virus which was discovered in the spring of 2012; the virus used some of the functionality first seen in Stuxnet.³² In other words, individual viruses may not be reusable, but that does not necessarily apply to cyberweapons as a class. Malware developers are increasingly using modular design to create sophisticated new viruses, with some interchangeable modules being borrowed from the existing malware, and others used as stand-alone products. The resulting viruses are extremely mutable—we are not saying infinitely mutable because there is only a finite number of zero-day vulnerabilities which malware writers have managed to identify and exploit.

It is therefore safe to say that with proper defenses it is possible to make sure that each individual virus can be used only once. Such a result can be achieved with proper management of IT systems, which require regular updates and timely maintenance. We also need to develop early warning instruments to nip cyberattacks in the bud; improve the existing approaches to the provision of cybersecurity; and strengthen cooperation between the governments and the commercial sector to ensure that software and hardware systems are updated in a timely manner. Let us look at whether and to what extent such measures have been used as part of the efforts to neutralize Stuxnet.

Initially the virus was studied by a very limited number of commercial cybersecurity labs and by the Industrial Control Systems Cyber Security Response Team (ICS-CERT). In subsequent months, cybersecurity experts described the team's response to such a serious threat as less than impressive. ICS-CERT failed to provide ICS operators with timely and specific recommendations about closing the vulnerabilities exploited by the virus.³³ It was only after the Stuxnet source code was made available on the Internet that research institutes and private experts joined the effort to study the virus. Only then did we have the first versions proposing which industrial control systems the virus was specific to, and which specific industrial facilities the perpetrators may have targeted. It is therefore safe to say that making the information about Stuxnet broadly available helped rather than hindered the effort to neutralize the virus.

Cybersecurity companies have also done quite a lot to study Stuxnet and to patch up the vulnerabilities in the Windows operating system. The first of those vulnerabilities were closed within a month of the virus being detected; most of them were fixed over the following several months. The companies which make anti-virus software, and the huge number of users running that software all over the world, were instrumental in tracking the geographical spread of the epidemic. It has been pointed out that any assessments of the infection rates in any given country can be made only if there are a sufficient number of anti-virus software users in that country.³⁴ Nevertheless, almost all cybersecurity companies tend to agree that the highest infection rates were seen in Iran, India, and Indonesia. Symantec, one of the leaders in this field, has released a detailed dossier on Stuxnet; it has become an excellent reference source for many experts who study the virus.

The global effort against Stuxnet depended on anti-virus software companies from the United States, Russia, Belarus, and other countries having their products installed on computers all over the world. But following the Stuxnet crisis Iran has stepped up efforts to develop its own anti-virus software.³⁵ In February 2012 it was reported that Tehran had banned imports of all cybersecurity products.³⁶ In future, that may severely reduce the amount of accurate technical information about newly discovered viruses which is available to specialist cybersecurity companies around the world.

In late May 2012 *Global Control*, a specialist journal, tested some of the leading anti-virus products to see how they cope with Stuxnet. It obtained a rather sobering set of results which may serve as an incentive to strengthen international cooperation in this area. None of the popular anti-virus products managed to detect all the existing versions of the virus, even though Stuxnet has been known for quite some time now.³⁷ How, then, can we expect any single company—even a national champion supported by the government—reliably to detect and cope with new, previously unknown versions of malicious software as sophisticated (or even more so) as Stuxnet? For that matter, how can we expect the same from any individual country or government?



It took numerous companies around the world, as well as the Iranian government, just under two years to eliminate all the hardware-level vulnerabilities in the Siemens ICS systems exploited by Stuxnet.³⁸ But with sufficient human and financial resources, a virus of that level of sophistication can be created from scratch in a matter of months. It might make sense to study the model which relies on open-source software and hardware in order to eliminate newly identified threats as quickly as possible.³⁹ Such a model would also spur competition and bolster the commercial sector's potential for innovation in the area of cybersecurity.

Be that as it may, now that we have analyzed the theories claiming that Stuxnet specifically targeted the nuclear infrastructure, we need to understand how these theories can contribute to the ongoing cybersecurity debate. Another question to answer is whether the existing template of the nuclear nonproliferation regime can be applied to the task of strengthening international cybersecurity and preventing the development of cyberweapons similar to the Stuxnet virus.

RELEVANCE OF NUCLEAR NONPROLIFERATION TO CYBERSECURITY

Efforts to build a nuclear nonproliferation regime commenced almost immediately after the first nuclear tests in 1945. Those efforts were pursued by a very narrow circle of sovereign states. Such an approach resulted primarily from the extremely high economic and technological threshold for the acquisition of nuclear weapons: at the time, only the most technologically advanced nations were capable of such a feat. First ideas about ways of preventing the spread of nuclear weapons were voiced as early as 1946. In the United States, the Acheson-Lilienthal Report argued that all military nuclear programs should be placed under international controls, and that peaceful programs should be subject to licensing and inspections.⁴⁰ The report highlighted uranium ore mining and production of fissile materials as the key elements of nuclear weapons proliferation.

By the early 1950s the number of known uranium deposits had grown substantially,⁴¹ so keeping them all under control was no longer feasible. Further efforts to establish a nuclear nonproliferation regime focused on preventing the spread of technologies for producing weapons-grade fissile materials. The manufacturing process was very energy-intensive and required a formidable industrial capability. To illustrate, in 1945 the energy consumption of the laboratory which produced fissile materials for the Manhattan Project was thrice the figure for Detroit, a large and highly industrialized city. At its peak the project employed about 12,000 people.⁴²

About a decade later the Soviet Union developed simpler and cheaper technologies which relied on gas centrifuges for uranium enrichment. In subsequent years a whole number of countries launched gas centrifuge programs: Israel and France in 1960, China in 1961, Australia in 1965, Sweden in 1971, Italy and India in 1972, Japan in 1973, and Brazil in 1979.⁴³ China, France, India, and Israel⁴⁴ ended up using those programs to acquire nuclear weapons.

The International Atomic Energy Agency (IAEA) was established in 1950 to prevent the spread of nuclear weapons technologies. The idea was that if any country wants to make use of peaceful nuclear energy but does not have the required technologies and expertise it can acquire both from the IAEA. In return, it must sign an agreement with the agency granting it the right to conduct on-site inspections in order to ascertain that the technologies are not being used to acquire nuclear weapons. But apart from institutions and codes of conduct, any international regime must also rely on norms and principles that regulate various interactions between the participants. These norms and principles were later incorporated in the Nuclear Non-Proliferation Treaty (NPT), which was signed in late 1960. This was followed by the introduction of controls over exports of sensitive technologies, including peaceful nuclear fuel cycle technologies which can potentially be used for weapons purposes.

Over the past decade the international community has made several steps to strengthen the nonproliferation regime. The United Nations has adopted Resolution 1540, which urges all member states to bring their national export control mechanisms into line with international standards. Other steps include the Proliferation Security Initiative and the launch (or strengthening) of several other financial and export control regimes.

Looking at this brief summary of the international community's nuclear nonproliferation efforts, one has to wonder whether that experience can be relevant to ensuring the security of cyberspace and preventing the proliferation of cyberweapons.

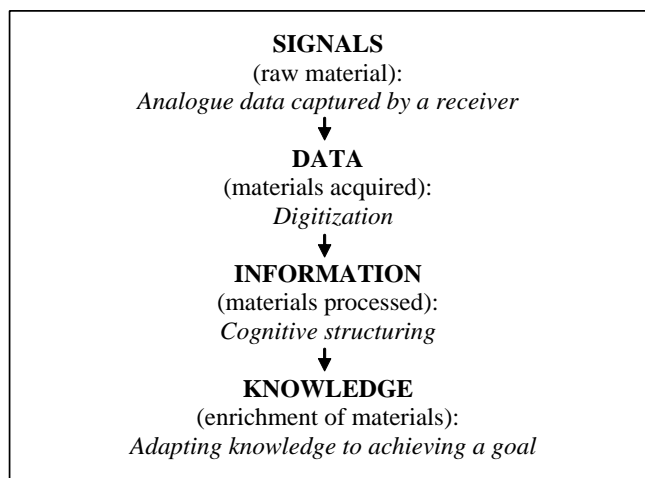
The starting point of nuclear weapon production is uranium ore. The process begins with uranium mining, and then goes through the stages of uranium ore processing, enrichment, and nuclear energy production. The starting point of the process which leads to the development of cyberweapons (which are essentially based on information) is signals. In order to become a cyberweapon, information signals have to undergo a series of transformations which in some ways resemble the enrichment of uranium (see Figure 1).⁴⁵

The first stage is to receive (acquire) the signal that will serve as source material for a cyberweapon. Then this signal—the data—undergoes cognitive structuring (processing) and turns into information. The stage of adapting the information to address a specific task (enrichment) is the most sensitive. In that sense it is similar to the nuclear enrichment stage, inasmuch as it determines whether the knowledge acquired as a result of that stage will be put to military or peaceful use. The choice can be made by an institution or an individual. If we are dealing with an institution, theoretically it is possible to establish some external controls over that choice. But if we are dealing with an individual, there are no technological instruments to make sure that knowledge is not transformed into a weapon. A cyberweapon is essentially knowledge which has been acquired and aggregated to achieve some specific goals in cyberspace through unilateral methods which amount to the use of force. If we accept that logic, it becomes clear that it is impossible to ban the production of cyberweapons—that would be tantamount to banning the production of knowledge in an information society.

This is why the existing experience of technological controls over the circulation of nuclear materials and technologies is not entirely relevant to preventing the proliferation of cyberweapons. But the experience of confidence-building measures and information exchange accumulated during the nuclear age can be used—or is being used already—to counter the existing challenges and threats to international information security. In particular, it is worth studying the experience of the national Nuclear Threat Centers, which facilitated the exchange of information about threats. Something akin to these centers has already been implemented in the shape of governmental and nongovernmental cyber emergency response groups. But the existing experience in the area of nuclear arms control is based primarily on bilateral interaction between the Soviet Union (Russia) and the United States. An effective international cybersecurity regime will require a multilateral approach, owing to the transnational nature of cyberspace itself; geographical gaps in the regime will render it ineffective. Finally, the existing nuclear nonproliferation experience does not answer the question of how to engage non-state actors in building the international information security regime.

All that being said, it would be premature to claim that the nuclear nonproliferation regime has already become fully mature, or that it has coped with all the pressing technological challenges.

Figure 1. Transformation of Signal into Knowledge



For example, there are still no proper international controls over uranium enrichment technologies. That is mainly because gas centrifuges are compact and easy to manufacture, and the line between their civilian and weapons uses is blurred. As a result, gas centrifuge technology has become an unprecedented challenge to the existing nonproliferation institutes.⁴⁶ Gas centrifuges are an integral element of peaceful nuclear energy infrastructure—but it is impossible to establish whether uranium is being enriched for civilian or weapons purposes without inspecting the nuclear facilities in question. One perfect example of this problem is the ongoing crisis over the Iranian nuclear program, which is centered on uranium enrichment, including at the Stuxnet-stricken Natanz facility.

The situation with Iran also highlights another important trend. The major nuclear cuts undertaken by the two nuclear superpowers in the 1990s gave renewed impetus to the nuclear nonproliferation regime—but now that impetus is beginning to fizzle out.⁴⁷ Further progress in the area of nuclear nonproliferation requires new measures, including multilateral nuclear disarmament steps.⁴⁸ But, as it so often happens, the things that have worked well for two partners do not necessarily work for five, let alone nine. New verification instruments will be required to ensure compliance with any future agreements on deeper nuclear cuts; the same applies to bans on nuclear tests and on the production of fissile materials for weapons purposes.

In other words, the existing nuclear nonproliferation regime and the future international information security regime share some common weaknesses. In particular, they are still lacking any social instruments for preventing the proliferation of nuclear and cyber weapons. Additionally, they both require a multilateral format for arms control (with participation not necessarily limited to state actors). It would therefore make a lot of sense for the communities of nuclear and IT specialists to pool their efforts and try to identify common solutions for all these problems. They could start, for example, by finding an answer to the question of whether civilian nuclear infrastructure facilities can be incorporated into the international information security regime.

Civilian nuclear infrastructure facilities require efforts on two fronts which can broadly be described as part of information security:

- ❑ on the one hand, they require measures to ensure the security of information as such (i.e. preventing the spread of sensitive information);
- ❑ on the other, they need physical security measures, i.e. steps to ensure the security of handling nuclear materials, and other elements of information systems on which the security of nuclear facilities depends.⁴⁹

Civilian nuclear infrastructure facilities include enrichment plants, laboratories, and nuclear research centers, research reactors, and nuclear power plants. Any failures in the information security systems at such facilities can result, first, in the leakage of sensitive nuclear information, and, second, in unacceptable social consequences. In countries where nuclear power accounts for a high proportion of the national energy balance (France, Japan, Ukraine, Germany, etc.) such failures can also cause serious economic problems and undermine the public's confidence in nuclear energy.⁵⁰

Information security systems at civilian nuclear facilities comply with the ISO 17799 (2000) standard, which is common for the entire IT sector. In 2005 specialists began to develop the updated ISO/IEC 27000 standard, which has received a positive assessment from the IAEA and will be used in the development of the principles of information security at civilian nuclear facilities. Another new standard is IEC 62645, which is currently being developed by the International Electrotechnical Commission. However, none of these standards takes into account the specifics of the nuclear industry in terms of the nuclear security requirements, including:⁵¹

- ❑ the lifecycle of civilian nuclear facilities, with different requirements to information security at different stages of that lifecycle;
- ❑ stringent requirements for the industrial control systems used at nuclear facilities, for the precision of calculations, and for reliability, compared with other IT systems;
- ❑ remote control centers, which enable operators to remain in control of the facility in the event of an emergency; these centers require additional communication channels—which can be vulnerable to interlopers;

- ❑ the need to develop highly reliable procedures for updating the software;
- ❑ the need for secure IT procurement procedures (guaranteeing the absence of any back doors which might be used to obtain unauthorized access);
- ❑ the need for inclusion in the terms of subcontracts of specific clauses to make sure that computer systems cannot be compromised by third parties.

In 2011 the IAEA Technical Working Group on Nuclear Power Plant Instrumentation and Control launched a coordinated research program (CRP) into security of digital instrumentation and control systems. As part of another initiative, the IAEA released several technical guidelines on information security. A report entitled *Technical Challenges and Solutions in Application of Digital I&C Systems in NPP* is to be published in 2013.

In and by themselves, technological measures will not be enough to counter cyberthreats; this goal also requires greater international cooperation. First steps in that direction were made in 2012. The final communiqué of the Nuclear Security Summit held in March 2012 in Seoul included a section which focused on information security at nuclear facilities. The document places heavy emphasis on measures to prevent the leakage of sensitive nuclear information, but has nothing to say about information threats to the security of nuclear facilities themselves. It refers to a resolution by the IAEA General Conference (GC(55)/Res/10) and ITU Resolution 174,⁵² which focus solely on protecting sensitive information. The same can be said about a presentation made by Kane Pollard, a representative of the British Embassy in Washington,⁵³ at the PONI Spring Conference in April 2012.⁵⁴

The IAEA believes that the threat of leakage of sensitive information is currently at low to medium severity level.⁵⁵ Meanwhile, the information threats to the security of nuclear facilities—i.e. the threats which actually pose the greatest danger—have not made it to the final communiqué. This is a shortcoming that needs to be addressed at the international level. A suitable platform for discussing this is the upcoming 2014 Nuclear Security Summit in the Netherlands.

Another important question is how to incorporate the security guarantees for civilian nuclear facilities into the international information security regime. Finding the right answers will require a broader debate on these problems among nuclear and IT experts. Such a debate can be launched at a suitable one-off event—but at some point it may require closer cooperation between the nuclear and IT communities, and proper institutionalization of such cooperation. The United States has already made some progress in this area. In 2009 the U.S. Department of Defense set up a special department for global strategic problems, tasked with drafting new policies on the prevention of WMD proliferation, nuclear and cyber security, and space-related problems. Russia could make use of that experience. At some point in the future such a mechanism could be tried at the international level, and the Russian leadership should work energetically for that to happen.

NEW PROBLEMS SHOULD BRING NEW OPPORTUNITIES

Stuxnet has brought a whole range of problems and scenarios to the forefront of international discussion concerning the future of the international information security regime. It has highlighted a complex interrelationship between digital and nuclear technologies. It has demonstrated that efforts to counter the threat posed by highly sophisticated malware require the involvement of not only states but also non-state actors. It has also drawn our attention to the fact that not only states, but private companies as well, may have the capabilities and motivation to create viruses such as Stuxnet. Finally, there is no denying that commercial cybersecurity labs have played a key role in neutralizing that virus. It has therefore become obvious that if we want to build an effective international information security regime we must take into account the constructive as well as destructive impact of non-state actors on the development of cyberweapons and of countermeasures against such weapons. That consideration alone explains why the future international information security regime and cyber-weapons controls cannot be a replica of the existing nuclear weapons controls, in which non-state actors continue to play a marginal role.

The second conclusion is that there are major differences between nuclear and cyber weapons in terms of their usage scenarios and identification of the attacker. Nuclear weapons have always




been viewed as an instrument that can be used only once. There has never been any possibility of doubt as to who wields those weapons, and identifying the attacker has never been seen as a problem. Without clear and unambiguous attribution of nuclear arsenals, the existing deterrence mechanisms would have been impossible. The Stuxnet attack, on the other hand, has highlighted the problem of identifying the attacker. Suspicions against the United States and Israel cannot be proven, and the number of other potential suspects is almost infinite. Meanwhile, new modifications and updated versions of the same virus continue to infect computers in different countries to this day. Cyberweapons assembled from interchangeable modules are like a hydra which keeps springing new heads, and infecting systems over and over again by exploiting new vulnerabilities. Such major differences between nuclear weapons and cyberweapons mean that the idea of directly replicating nuclear arms control and nonproliferation mechanisms in cyberspace (the cyber-IAEA proposal by Evgeny Kaspersky) has limited utility.

At the same time, it is becoming clear that the future international information security regime must focus on making it impossible for each individual cyberweapon to be used more than once. The protracted battle against Stuxnet has highlighted the urgent need for international mechanisms of early detection of cyberattacks, and for global early warning systems. It has also demonstrated that private companies must be engaged in building up global defenses against cyberweapons as part of centralized international platforms, such as the UN.

On the other hand, the Stuxnet case has been yet another demonstration of the fact that the nuclear nonproliferation regime and the future international information security regime also have a lot of important things in common. One of them is the need for a multilateral format. The diffusion and falling costs of nuclear technologies are lowering the entry barriers for nuclear programs, and the nuclear-weapon states are waging an increasingly desperate battle against proliferation. The dialogue on nuclear arms control, which used to be the exclusive domain of the two superpowers and their allies, is turning into a multilateral discussion, in which every country's voice is important. The need for such a multilateral format is even more obvious when talking about information security; after all, most countries already have the capability to develop cyberweapons. In other words, the nuclear nonproliferation regime cannot be used as a direct template for the international information security regime—but it still offers valuable experience of multilateral solutions and approaches.

In addition, the experience accumulated in the area of arms control can be used in the development of social mechanisms for providing international information security. We need instruments to prevent the leakage of sensitive knowledge about software and cybersecurity systems—in the same way as there are mechanisms to prevent the leakage of sensitive nuclear know-how. Nuclear nonproliferation is gradually losing momentum, and the regime itself is approaching a point where sustaining it will require new mechanisms to be developed and put into practice. In view of the many similarities between the nuclear and IT spheres, it is safe to assume that cooperation between the two expert communities would enable them to identify more effective solutions and exploit synergies in overcoming the challenges to nuclear and information security. The potential institutional platforms for such cooperation include the 2014 Nuclear Security Summit in the Netherlands, and similar events.

One final topic for discussion should be security guarantees for civilian nuclear infrastructure as part of the international information security regime. There are several good reasons why nuclear facilities should not be lumped together with all other critical infrastructure; some of those reasons have been demonstrated by Stuxnet. The issue therefore deserves to be given a separate line on the international information security agenda. Russia, meanwhile, should study other countries' experience and start making progress in this area by establishing standing bodies in charge of the information security of the country's vast nuclear infrastructure. 

NOTES

¹ VirusBlockada also has an office in Moscow and a license to operate from the Federal Service for Technical and Export Control. See: <http://www.virusblokada.ru/about/>, last accessed January 15, 2013.

² N. Falliere, L. Murchu and E. Chien, "W32.Stuxnet Dossier," V1.4. Symantec, February 2011, http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf, last accessed January 15, 2013.

- ³ A. Gostev, "Myrtle and Guava: An Epidemic in Progress," 2010, <http://www.securelist.com/ru/blog/34361/Mirt_i_guava_Epidemiya_v_dinamike>, last accessed January 15, 2013.
- ⁴ Siemens International, "SIMATIC PCS 7: Information about Malware. Handling Stuxnet," Industry Online Support, <<http://support.automation.siemens.com/WWW/adsearch/resultset.aspx?region=VW&lang=en&netmode=internet&ui=NDawMDAxNwAA&term=stuxnet&ID=43876783&ehbid=43876783>>, last accessed January 15, 2013.
- ⁵ K. Benedict, "Stuxnet and the Bomb," *The Bulletin*, 2012, June 15, <<http://thebulletin.org/web-edition/columnists/kennette-benedict/stuxnet-and-the-bomb>>, last accessed January 15, 2013.
- ⁶ U.S. Department of Defense, "Department of Defense Strategy for Operating in Cyberspace," July 2011, <<http://www.defense.gov/news/d20110714cyber.pdf>>, last accessed January 15, 2013.
- ⁷ E. Kaspersky, "Net voine! Nota bene. Evgeny Kaspersky Talks about the Interesting, the Pleasant and the Urgent," November 21, 2011, <<http://eugene.kaspersky.ru/2011/11/25/net-voine/>>, last accessed January 15, 2013.
- ⁸ R. Langner, "Our Stuxnet Timeline," December 9, 2010, <<http://www.langner.com/en/2010/12/09/our-stuxnet-timeline/>>, last accessed January 15, 2013.
- ⁹ R. Langner, "Stuxnet is a Directed Attack—Hack of the Century," September 13, 2010, <<http://www.langner.com/en/2010/09/13/stuxnet-is-a-directed-attack-hack-of-the-century/>>, last accessed January 15, 2013.
- ¹⁰ The author has run Google searches for "stuxnet" and "stuxnet Bushehr," using the first 100 results displayed. Search statistics for the periods between September 1–September 20, 2010, and September 21–October 21, 2011 indicate that the number of mentions of Stuxnet began to rise starting from September 21, 2010.
- ¹¹ BBC, "Stuxnet Worm Hits Iran Nuclear Plant Staff Computers," 2010, September 26, <<http://www.bbc.co.uk/news/world-middle-east-11414483>>, last accessed January 15, 2013.
- ¹² P. Hafezi, "Iran says Bushehr Nuclear Plant not Damaged by Stuxnet," Reuters, September 27, 2010, <<http://www.reuters.com/article/2010/09/27/us-iran-cyber-bushehr-idUSTRE68Q39Z20100927>>, last accessed January 15, 2013.
- ¹³ D. Brunnstrom and L. Ireland, "Russia Says Stuxnet Could Have Caused New Chernobyl," Reuters, 2011, January 26, <<http://www.reuters.com/article/2011/01/26/us-iran-nuclear-russia-idUSTRE70P6WS20110126>>, last accessed January 15, 2013.
- ¹⁴ Y. Melman, "Computer Virus in Iran Actually Targeted Larger Nuclear Facility," *Haaretz*, September 28, 2010, <<http://www.haaretz.com/print-edition/news/computer-virus-in-iran-actually-targeted-larger-nuclear-facility-1.316052>>, last accessed January 15, 2013.
- ¹⁵ Falliere et al., op. cit.
- ¹⁶ J. Carr, "Stuxnet's Finnish–Chinese Connection," *Forbes*, December 14, 2010, <<http://www.forbes.com/sites/firewall/2010/12/14/stuxnets-finnish-chinese-connection/>>, last accessed January 15, 2013.
- ¹⁷ D. Albright, P. Brannan and C. Walrond, "Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant? Preliminary Assessment," ISIS, December 22, 2010, <<http://isis-online.org/isis-reports/detail/did-stuxnet-take-out-1000-centrifuges-at-the-natanz-enrichment-plant>>, last accessed January 15, 2013.
- ¹⁸ D. Albright and C. Walrond, "Iran's Gas Centrifuge Program: Taking Stock," ISIS, February 11, 2010, <<http://isis-online.org/isis-reports/detail/irans-gas-centrifuge-program-taking-stock>>, last accessed January 15, 2013.
- ¹⁹ P. Hafezi, "Iran Admits Cyber Attack on Nuclear Plants," Reuters, November 29, 2010, <<http://www.reuters.com/article/2010/11/29/us-iran-idUSTRE6AS4MU20101129>>, last accessed January 15, 2013.
- ²⁰ D. Albright, P. Brannan and C. Walrond, "Stuxnet Malware and Natanz: Update of ISIS December 22, 2010 Report," ISIS, February 15, 2011, <<http://isis-online.org/isis-reports/detail/stuxnet-malware-and-natanz-update-of-isis-december-22-2010-reportsupa-href1/>>, last accessed January 15, 2013.
- ²¹ R. Langner, "Enumerating Stuxnet's Exploits," June 7, 2011, <<http://www.langner.com/en/2011/06/07/enumerating-stuxnet%E2%80%99s-exploits/>>, last accessed January 15, 2013.
- ²² D. Sanger, "Obama Order Sped Up Wave of Cyberattacks Against Iran," *New York Times*, June 1, 2012, <http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?_r=1&pagewanted=all>, last accessed January 15, 2013.
- ²³ "Iran increases number of uranium enrichment centrifuges to 9,000," *Ukrainews*, February 15, 2012. <<http://ukranews.com/ru/news/world/2012/02/15/64131>>, last accessed January 15, 2013.



- ²⁴ Falliere et al., op. cit.
- ²⁵ A. Matrosov, E. Rodionov, D. Harley and J. Malcho, “Stuxnet Under the Microscope Revision 1.1,” ESET, 2010, <http://eset.ru/company/viruslab/analytics/doc/Stuxnet_Under_the_Microscope.pdf>, last accessed January 15, 2013.
- ²⁶ “NSTB Assessments Summary Report: Common Industrial Control System Cyber Security Weaknesses,” DOE Idaho Operations Office, May 2010, <<http://www.fas.org/sgp/eprint/nstb.pdf>>, last accessed January 15, 2013.
- ²⁷ M. Edwards and T. Stauffer, “Control System Security Assessments,” 2008 Siemens Automation Summit, <<http://graphics8.nytimes.com/packages/pdf/science/NSTB.pdf>>, last accessed January 15, 2013.
- ²⁸ B. Schneier, “Cyberwar,” June 4, 2007, <<http://www.schneier.com/blog/archives/2007/06/cyberwar.html>>, last accessed January 15, 2013.
- ²⁹ J. Carr, “Dragons, Tigers, Pearls, and Yellowcake: 4 Stuxnet Targeting Scenarios,” November 16, 2010, <http://nanojv.files.wordpress.com/2011/03/dragons_whitepaper_updated1.pdf>, last accessed January 15, 2013.
- ³⁰ J. Brito and T. Watkins, “Loving the Cyber Bomb? The Dangers of Threat Inflation in Cybersecurity Policy,” Mercatus Center at George Mason University, April 2011, <<http://jerrybrito.com/pdf/3HNSJ39.pdf>>, last accessed January 15, 2013.
- ³¹ M. Libicki, “Pulling Punches in Cyberspace,” in Proceedings of a Workshop on Deterring Cyberattacks. Informing Strategies and Developing Options for U.S. Policy, National Academy of Sciences, 2010, <http://www.nap.edu/openbook.php?record_id=12997&page=123>, last accessed January 15, 2013.
- ³² For more details, see: O. Demidov and M. Simonenko, “Flame in Cyberspace,” *Security Index*, No. 4 (Fall 2012).
- ³³ D. Peterson, “ICS-CERT: Stuxnet Lessons Learned,” *Digital Bond*, 2010, <<http://www.digitalbond.com/2010/10/22/ics-cert-stuxnet-lessons-learned/>>, last accessed January 15, 2013.
- ³⁴ A. Gostev, “Myrtle and Guava: Epidemic in Progress,” 2010, <http://www.securelist.com/ru/blog/34361/Mirt_i_guava_Epidemiya_v_dinamike>, last accessed January 15, 2013.
- ³⁵ S. Isayev and T. Jafarov, “Iran Starts Making Own Anti-virus Software,” *Trend*, May 3, 2012, <<http://en.trend.az/regions/iran/2021650.html>>, last accessed January 15, 2013.
- ³⁶ S. Isayev and T. Jafarov, “Iran Bans Import of Foreign Computer Security Software,” *Trend*, February 20, 2012, <<http://en.trend.az/regions/iran/1994160.html>>, last accessed January 15, 2013.
- ³⁷ “What’s the Best Defense Against Stuxnet? A Comparison of Which Tools Are the Best for Finding Stuxnet in a System,” May 28, 2012, <<http://www.controlglobal.com/articles/2012/stuxnet-iranian-view.html?page=full>>, last accessed January 15, 2013.
- ³⁸ D. Peterson, “Stuxnet Clock Stops At 625 Days,” *Digital Bond*, May 31, 2012, <<http://www.digitalbond.com/2012/05/31/stuxnet-clock-stops-at-625-days/>>, last accessed January 15, 2013.
- ³⁹ W. Clark and P. Levin, “Securing the Information Highway,” *Rossiya v globalnoy politike*, No. 3 (2010), <<http://www.globalaffairs.ru/numbers/74>>, last accessed January 15, 2013.
- ⁴⁰ *The Acheson-Lilienthal Report: Report on the International Control of Atomic Energy* (Washington, D.C.: U.S. Government Printing Office, 1946), <<http://www.learnworld.com/ZNW/LWTText.Acheson-Lilienthal.html>>, last accessed January 15, 2013.
- ⁴¹ “NPT Briefing Book,” Centre for Science & Security Studies, James Martin Center for Nonproliferation Studies, Monterey Institute of International Studies, 2012, <<http://www.kcl.ac.uk/sspp/departments/warstudies/research/groups/csss/2012nptbook.pdf>>, last accessed January 15, 2013.
- ⁴² *AEC Handbook on Oak Ridge* (Oak Ridge National Laboratory, 1955).
- ⁴³ R. Kemp, “Centrifuges: A New Era for Nuclear Proliferation,” Nonproliferation Policy Education Center Monograph, 2012, <http://npolicy.org/article_file/Centrifuges_A_new_era_for_nuclear_proliferation.pdf>, last accessed January 15, 2013.
- ⁴⁴ Tel Aviv neither confirms nor denies possession of nuclear weapons. Officially, Israel is not a nuclear-weapon state.
- ⁴⁵ J. Rowley, “The Wisdom Hierarchy: Representations of the DIKW Hierarchy,” *Journal of Information Science*, No. 33 (2007), pp. 163–180, <<http://jis.sagepub.com/content/33/2/163.abstract>>, last accessed January 15, 2013.
- ⁴⁶ Kemp, “Centrifuges: A New Era for Nuclear Proliferation.”

- ⁴⁷ J. Acton, "Low Numbers: A Practical Path to Deep Nuclear Reductions," Carnegie Endowment for International Peace, 2011, <http://carnegieendowment.org/files/low_numbers.pdf>, last accessed January 15, 2013.
- ⁴⁸ S. Lavrov, "The New START Treaty in the Global Security Matrix," *Mezhdunarodnaya Zhizn*, No. 7 (July 2010).
- ⁴⁹ This is based on classification contained in the IAEA technical guidelines document *Computer Security at Nuclear Facilities*, released in 2011. The classification was simplified and adapted for the purposes of this article.
- ⁵⁰ "Announcement of a New IAEA Co-ordinated Research Programme (CRP. IAEA, 2011)," <<http://www.iaea.org/NuclearPower/Downloads/Engineering/meetings/2011-05-TWG-NPPIC/CRP-CyberSecurity.pdf>>, last accessed January 15, 2013.
- ⁵¹ "Computer Security at Nuclear Facilities," IAEA Nuclear Security Series No. 17, 2011, <http://www-pub.iaea.org/MTCD/Publications/PDF/Pub1527_web.pdf>, last accessed January 15, 2013.
- ⁵² "Seoul Communiqué," Seoul Nuclear Security Summit, 2012, <http://www.thenuclearsecuritysummit.org/userfiles/Seoul%20Communique_FINAL.pdf>, last accessed January 15, 2013.
- ⁵³ Britain was the author of proposals to include a section on information security in the final communiqué of the 2012 Nuclear Security Summit in Seoul.
- ⁵⁴ K. Pollard, "The UK Contribution to the 2012 Nuclear Security Summit," British Embassy in Washington, D.C. 2012, <https://csis.org/images/stories/poni/120417_Pollard.pdf>, last accessed January 15, 2013.
- ⁵⁵ "Computer Security at Nuclear Facilities," IAEA Nuclear Security Series No. 17, 2011, <http://www-pub.iaea.org/MTCD/Publications/PDF/Pub1527_web.pdf>, last accessed January 15, 2013.





ABOUT THE AUTHORS

Antonov, Anatoly, Dr., is Deputy Minister of Defense of the Russian Federation, Ambassador Extraordinary and Plenipotentiary. In 1978 graduated from the Moscow State Institute of International Relations. He served for the Ministry of Foreign Affairs (MFA) of the USSR and Russia in various positions at central office and abroad over 30 years. Since 2004 – Director of the Department for Security Affairs and Disarmament of the MFA. He has broad experience in negotiation process. He was a head of Russian government delegations at negotiations on the Treaty on Non-proliferation of Nuclear Weapons, Review of Inhumane Weapons Convention, Elimination of Chemical Weapons Convention, Elimination of Biological Weapons Convention, and Treaty on Strategic Offensive Arms. He was the head of Russian delegation at the talks on new START treaty. On February 2011 he was appointed as Deputy Minister of Defense of the Russian Federation. Since 2010 – Member of the Sustainable Partnership with Russia Group.

Baklitsky, Andrey, is PIR Center Internet Project Director. PhD student at the Institute of Oriental Studies of the Russian Academy of Sciences. Graduated from the Faculty of the International Relations of the Urals Federal University. Holds specialist degree in regional studies and simultaneous interpreter diploma. In the years 2008–2009 took a course at the University of Seville (Spain). The Russian Center for Policy Studies (PIR Center) intern in May–July, 2011. E-mail address: baklitsky@pircenter.org

Buzhinsky, Evgeny, Lieut.-Gen., is the PIR Center Senior Vice President, the former Head of the International Treaty Directorate, Deputy Head of the Main Department of International Military Cooperation of the Russian Defense Ministry (2002–2009). Graduated from the Military Institute, Frunze Military Academy. In 1976–1992 – served in different positions as officer of the General Staff. In 1992–2009 – served in the Department of the International Treaty Directorate of the Main Department of International Military Cooperation of the Russian Defense Ministry. In 2002 he was appointed on the position of the Head of the International Treaty Directorate. PIR Center Advisory Board member. Sustainable Partnership with Russia (SuPR) Group member. E-mail address: buzhinsky@pircenter.org

Demidov, Oleg, is Coordinator of PIR Center International Information Security and Global Internet Governance Project. Graduated from School of Public Administration of Moscow State University. In 2006–2009 completed additional specialization program in Higher School of Translation and Interpretation in Moscow State University. Currently is a postgraduate student at the Department of political science at Moscow State Institute of International Relations. The dissertation's thesis deals with the influence of transnational actors on armed conflicts in the region of North Caucasus. Previously held the position of Project Coordinator at the Center of Political and International Studies (CPIS). E-mail address: demidov@pircenter.org

Kasayev, Eldar, is an expert on international law. In 2008 he graduated the International Institute of Energy Policy and Diplomacy at the MGIMO University. He is the author of over 50 publications on the Middle East and North Africa. The areas of academic interests include legal aspects of subsoil use, investment climate, prospects of the Russian companies in the Middle East and North Africa (Iran, Iraq, Qatar, Kuwait, Algeria, and Libya). In 2006 he conducted research for *Rosneft* on



analysis of political, economic and legal risks in a number of the Middle East and North African countries. E-mail address: eldar_karach@mail.ru

Kmentt, Alexander, Amb., is Director for Disarmament and Non-Proliferation, Austrian Federal Ministry for European and International Affairs. He has previously served as a Special Assistant to the Executive Secretary of Preparatory Commission for the Comprehensive Nuclear-Test-Ban Treaty Organization (CTBTO). Previous disarmament responsibilities in the Austrian Foreign Ministry include Deputy Permanent Representative of Austria to the Conference on Disarmament in Geneva and Deputy Director for Disarmament Affairs. During the Austrian EU Presidency in 2006, he chaired the EU Working Group on Non-Proliferation. Alexander Kmentt holds a Law Degree from the University of Graz and a Masters Degree in International Relations from Cambridge University, UK.

Kolbin, Alexander, is PIR Center Russia and Nuclear Nonproliferation Program Coordinator. In April–June 2012 – visiting researcher at the Stockholm International Peace Research Institute (SIPRI) working on transparency issue within the context of nuclear disarmament process. In 2011 graduated from Tomsk State University, Faculty of History, Department of Modern and Contemporary History and International Relations. In 2010 – PIR Center intern specializing on China's nuclear strategy. Participant of the 2010 PIR Center International Summer School on Global Security. E-mail address: kolbin@pircenter.org

Leclercq, Arnaud, is Head of New Markets Division and Member of the Executive Board of the Swiss private bank *Lombard Odier*. Completed business law studies, holds an MBA from HEC Paris and is a graduate of the Harvard Business School. He began his career in 1989 at the Paris law firm Berlioz where he specialized in M&A in emerging countries. In 1991, he founded his own consulting firm in Moscow. After selling it in 1994, he held various international positions in Bouygues Group. In 2000 he joined *Credit Suisse*, later becoming Managing Director and member of several Boards. Arnaud Leclercq joined *Lombard Odier* on July 1, 2006, and became a Partner of *Lombard Odier* Capital Partners on January 1, 2007. Winner in 2007 of the “Outstanding Young Private Banker Europe” by the Gobal Awards in Singapore. The author of the book “La Russie, puissance d’Eurasie, Histoire géopolitique des origines à Poutine” (Russia as the Eurasian Power. Geopolitical History from the Origins to Putin).

Luzin, Pavel, Dr., is a lecturer in the Department of the World History in the Perm State National Research University and the Department of the Liberal Arts in the Higher School of Economics (Perm, Russia), PIR Center expert. In 2008 he has undertaken an internship at PIR Center; also he was an alumnus of PIR Center International Summer School on Global Security 2008. In 2009 he was an employee in the Office of Perm region to the Government of the Russian Federation. In 2008–2011, he made his PhD studies at the Institute of the World Economy and International Relations, Russian Academy of Sciences. E-mail address: pavel.luzin@gmail.com

Murogov, Viktor, Dr., is Director of International Center for Nuclear Education, MEPHl (Moscow, Russia), Professor of State Technical University of Nuclear Power (Obninsk, Russia), Chief Scientist of Russian Research Centre Kurchatov Institute (Moscow, Russia), Director of Russian Association Nuclear Science and Education (RANSE). Graduated from Moscow Institute of Physics and Engineering in 1961. In 1989 he received Doctor's degree in Nuclear Physics. From 1996 to 2004 the Deputy General Director of International Atomic Energy Agency (IAEA) and represented the Russian Federation in IAEA. During this period he also worked as the Head of Department of Nuclear Energy of IAEA, General Manager of IAEA MP 1 – “Nuclear Power, Fuel Cycle and Nuclear Science”. In 2000–2003 a Project Manager for the NPRO International Project. PIR Center Advisory Board member. E-mail address: murogov@iate.obninsk.ru

Orlov, Vladimir, Dr., is the founder and the President of the PIR Center – the Russian Center for Policy Studies and the Editor-in-Chief of the *Security Index* journal. Graduated from the Moscow State Institute of International Affairs (MGIMO). Dr. Orlov is a member of the Public Board at the Ministry of Defense of the Russian Federation. He is 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 of the *Dialogue* Club International which he founded in 1993, a member of the *Washington Quarterly* Editorial Board. Dr. Orlov is Associate Research Fellow at GCSP. In 2001–2002 he served as UN consultant on disarmament and nonproliferation education by appointment of the UN Secretary General. During the 2010 NPT Review Conference he served as

a member of the official delegation of the Russian Federation. Dr. Orlov 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. Dr. Orlov continues to teach on a regular basis, giving lectures on Russian foreign policy and WMD nonproliferation. E-mail address: orlov@pircenter.org

Saunders, Jamie, the United Kingdom Foreign and Commonwealth Office Director for International Cyber Policy (UK). He took up this post in January 2012, following over 20 years of security policy experience. His most recent assignment was as cyber policy lead in the British Embassy, Washington (2008–2011). Previously he was assigned to a range of operational and policy positions at the UK's Government Communications HQ.

Simonenko, Maxim, is Master Student at the National Research University Higher School of Economics (Moscow, Russia). Graduated from the Tomsk State University, International Relations Department. Participant of the IV (2009) and V (2010) Summer Schools on Nuclear Non-proliferation organized by the Tomsk State University and Swedish Radiation Safety Authority. His scientific interests include world politics, nuclear non-proliferation, conflicts in cyberspace, Internet governance. E-mail address: simonenko.maksim@gmail.com

Spassky, Nikolay, is a Deputy Director General of Russia's Nuclear Energy State Corporation *Rosatom*. Member of the *Security Index* Editorial Board. Graduated from the Moscow State Institute of International Relations in 1983. Worked in various diplomatic positions within the Ministry of Foreign Affairs, including Deputy and First Deputy Director (1992–1994); Director of the North America Department (1994–1995); Member of the Ministry of Foreign Affairs Board (1995–1998); Joint Russian Ambassador to Italy and San Marino (1998–2004); Assistant Secretary to the Russian Security Council (2004–2006). PhD in Political and Historical Sciences. Envoy Extraordinary and Minister Plenipotentiary.

Zinovyeva, Elena, Dr., is a Senior Lecturer in the Department of Global Political Processes, MGIMO University (Moscow, Russia). From 2007–2008, she was a staff member at the Center for Internet Politics at MGIMO. From 2009–2011, she headed the project "The Dynamics of world political development and Russia's global competitiveness" at Russia's Ministry of Education and Science, Research and Education Center at MGIMO. Since 2012, has been head of the project "Theory and Practice of Intercultural Engagement in the Context of European Security" as well as "Socio-Psychological Analysis of Russian Research Culture, based on data from Russian research funds." E-mail address: ezinovyeva@hse.ru 