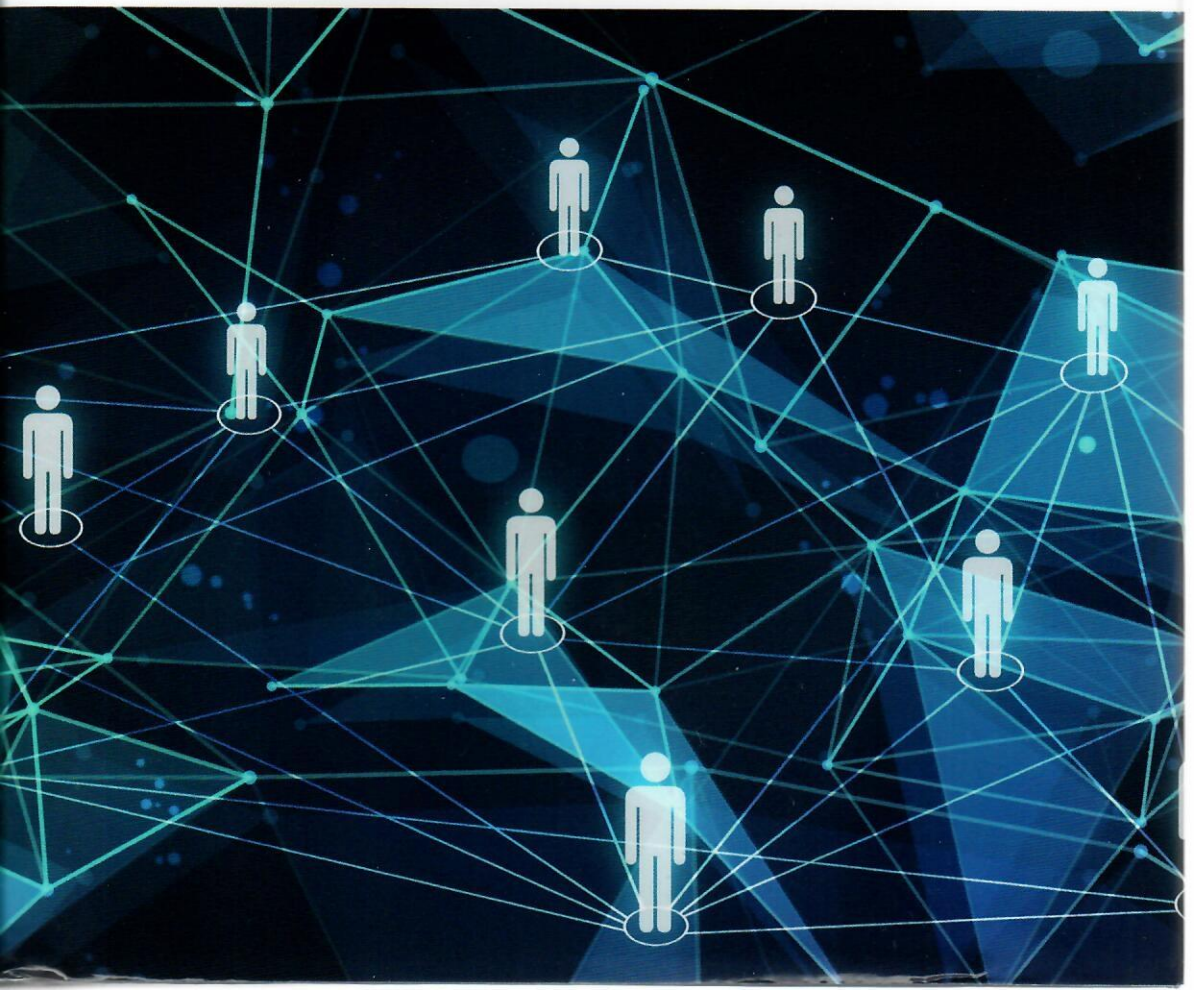
Preventing Black-Market Trade in Nuclear Technology

Edited by Matthew Bunn, Martin B. Malin, William C. Potter, and Leonard S. Spector



Preventing Black-Market Trade in Nuclear Technology

Edited by

MATTHEW BUNN
Harvard University

MARTIN B. MALIN
Harvard University

WILLIAM C. POTTER
Middlebury Institute of International Studies at Monterey

LEONARD S. SPECTOR
Middlebury Institute of International Studies at Monterey

CAMBRIDGE
UNIVERSITY PRESS

CAMBRIDGE
UNIVERSITY PRESS

University Printing House, Cambridge CB2 8BS, United Kingdom

One Liberty Plaza, 20th Floor, New York, NY 10006, USA

477 Williamstown Road, Port Melbourne, VIC 3207, Australia

314–321, 3rd Floor, Plot 3, Splendor Forum, Jasola District Centre,
New Delhi – 110025, India

79 Anson Road, #06–04/06, Singapore 079906

Cambridge University Press is part of the University of Cambridge.

It furthers the University's mission by disseminating knowledge in the pursuit of education, learning, and research at the highest international levels of excellence.

www.cambridge.org
Information on this title: www.cambridge.org/9781107163768
DOI: 10.1017/9781316681671

© Cambridge University Press 2018

This publication is in copyright. Subject to statutory exception and to the provisions of relevant collective licensing agreements, no reproduction of any part may take place without the written permission of Cambridge University Press.

First published 2018

Printed in the United States of America by Sheridan Books, Inc.

A catalog record for this publication is available from the British Library.

Library of Congress Cataloging-in-Publication Data
NAMES: Bunn, Matthew, editor.
TITLE: Preventing black-market trade in nuclear technology / edited by Matthew Bunn [and three others].
DESCRIPTION: Cambridge, United Kingdom ; New York, NY : Cambridge University Press, 2018. | Includes index.
IDENTIFIERS: LCCN 2017032441 | ISBN 9781107163768 (hardback)
SUBJECTS: LCSH: Nuclear nonproliferation. | Illegal technology transfers.
CLASSIFICATION: LCC JZ5687 .P74 2018 | DDC 327.1/747–dc23
LC record available at https://lccn.loc.gov/2017032441

ISBN 978-1-107-16376-8 Hardback

Cambridge University Press has no responsibility for the persistence or accuracy of URLs for external or third-party internet websites referred to in this publication and does not guarantee that any content on such websites is, or will remain, accurate or appropriate.

Contents

Contributors *page* vii

Acknowledgments ix

1 Introduction: The Problem of Black-Market Nuclear Technology Networks 1
Matthew Bunn and William C. Potter

2 The World of Illicit Nuclear Trade: Present and Future 23
David Albright and Andrea Stricker

3 The Role of Intelligence in Countering Illicit Nuclear-Related Procurement 48
Thomas Fingar

4 Strengthening the Global Law-Enforcement Response 79
Leonard S. Spector

5 Strengthening Sanctions and Interdiction 110
Mark Fitzpatrick

6 Strengthening Global Nuclear Export Controls 140
Ian Anthony

7 The Private Sector's Role in Stopping Black-Market Nuclear Technology Networks 159
Robert Shaw

8 Strengthening Global Nonproliferation Financial Controls 185
Justine Walker

9 Strengthening the Role of International Organizations in Dealing with Illicit Nuclear Technology Networks 209
Olli Heinonen

10 Countering Nuclear Black Markets by Strengthening Nonproliferation Culture 249
Matthew Bunn

11 Stopping Black-Market Nuclear Technology Networks: A View from Russia 271
Vladimir A. Orlov and Oleksandr Cheban

12 Out-of-the-Box Initiatives to Combat Illicit Nuclear Technology Procurement Networks 301
John Park, Leonard S. Spector, Ian J. Stewart

13 Conclusion: Stopping Illicit Trade in Nuclear Technology: Progress, Gaps, and Next Steps 323
Martin B. Malin, Matthew Bunn, Leonard S. Spector, William C. Potter

Index 365

11

Stopping Black-Market Nuclear Technology Networks

A View from Russia

Vladimir A. Orlov and Oleksandr Cheban

INTRODUCTION

When a product is in high demand and governments try to restrict its availability, there will always be a black market for it. Such black markets have destabilizing effects on the economy and society. The situation becomes especially threatening when the product in question is nuclear materials or nuclear technologies.

The nuclear technology black market is not among Russia's most pressing concerns at the moment – unlike, for example, the problem of drug trafficking. Nevertheless, there is still a danger of technologies or equipment that can be used to develop and build nuclear weapons falling into the wrong hands. This chapter therefore aims to analyze the Russian position with regard to the nuclear technology situation in Russia itself, as well as with regard to the international nuclear black market.

This chapter will look back at the situation that existed in the 1990s and 2000s before analyzing the current state of affairs. The background section will mostly focus on whether there have been any leaks of nuclear technologies or equipment from Russia that could contribute to nuclear weapons programs. The contemporary section will include a review of Russian legislation and regulation pertaining to the suppression of the nuclear black market, as well as practical efforts to enforce these laws. It will also focus on the Russian export-control system, especially so-called internal compliance programs (intra-corporate controls). Finally, the chapter will analyze Russia's official stance with regard to international efforts against the nuclear black market.

THE NUCLEAR TECHNOLOGY MARKET IN RUSSIA, 1992–2012

In the 1990s, which was a very difficult period for Russia, leaks of nuclear technology were as worrying as the trafficking in nuclear materials and remain a serious concern to this day. Incidents of nuclear technology leaks from Russia in the 1990s were not properly investigated because nuclear materials theft was seen as a more important priority. Nevertheless, we have several examples demonstrating that the risks of nuclear technology and equipment proliferation really did exist at the time, causing real as well as imaginary concerns.

The most high-profile example of nuclear technology proliferation is the so-called Mikhaylov Protocol. In this case, the proliferation threat arose not from a clandestine procurement network, but in an official initiative of the Russian government. On January 8, 1995, the then Russian nuclear energy minister, Viktor N. Mikhaylov, signed a protocol with the Iranian government on the completion of the No. 1 reactor of the Bushehr nuclear power plant. Under the terms of that protocol, which was signed during the minister's visit to Iran, Russia was to supply a 30–50 MW light water research reactor and build other research reactors in that country. Russia was also to provide assistance in the exploration of a uranium deposit in Iran, in building a centrifuge uranium-enrichment facility, and in training Iranian nuclear specialists in Russia. The value of the deal was estimated at $800 million.[1]

Western experts and politicians sharply criticized the protocol because they already suspected Iran sought to acquire nuclear weapons. There were even some domestic criticisms in Russia itself.[2] It remains unclear, however, whether these criticisms were entirely justified.[3] The most reasonable worries were expressed about the clause under which Russia was

[1] Aleksey Yablokov, "Nekotorye voprosy po povodu atomnoi sdelki s Iranom [Some Questions About the Nuclear Deal with Iran]," *Yaderny Kontrol*, no. 5 (May 1995), p. 20, http://pircenter.org/media/content/files/9/13464096210.pdf.

[2] For example, writing in *Yaderny Kontrol*, Professor Yablokov expressed concerns that the training of Iranian specialists in Russia could give them nuclear weapons know-how. See: Yablokov, "Nekotorye voprosy po povodu atomnoi sdelki s Iranom."

[3] As David Fischer, former Deputy Director General of the IAEA, rightly noted in response to an article by Yablokov, Iran already had a large number of high-caliber nuclear physicists in the 1990s. They were trained as part of the nuclear program which Iran pursued under the Shah. Most of them left Iran after the 1979 Islamic Revolution, but in the 1990s the Iranian government did everything it could to encourage their return. In any event, as David Fischer pointed out, it is impossible to ban nuclear physics education and

to help Iran build a centrifuge uranium-enrichment plant. However, that particular clause, which posed the biggest danger to the nonproliferation regime, was eventually removed from the document. This was done after intense US pressure, at a Clinton–Yeltsin summit. Mikhaylov himself (and his team at Minatom) did not see the sale of centrifuge technology and other sensitive items as anything special or controversial and they did not agree it posed significant proliferation risks.[4]

Although the United States placed enormous pressure on Russia at that time, Russia's decision to undo the most sensitive and controversial parts of its almost agreed deal with Iran was primarily the result not of external pressures but of an intense inter-agency review of the situation. Russian inter-agency meetings resulted in the understanding that any sensitive nuclear shipments to Iran would be undesirable for Russia and would not serve Russia's national interests. It is worth noting that during 1995, it is now known, Iran was accelerating its clandestine uranium-enrichment program pursuant to a 1994 agreement with the A. Q. Khan network, which included delivery of designs and components for 500 first-generation uranium-enrichment centrifuges and design documents for next-generation P-2 centrifuge units.[5] It is not known whether information regarding this transaction came to Moscow's attention and led to its decision to pull back from Mikhaylov's offer of a centrifuge enrichment plant.

Although the Mikhaylov Protocol ultimately did not result in the transfer of proliferation-sensitive technology, stresses brought on by the break-up of the Soviet Union and instability in the Russian economy did lead to other episodes of leakage of proliferation-relevant Russian technology. The most high-profile missile technology leak was the export of gyroscopes (which are used in missile homing systems) to Iraq by the

training. Such a ban would be as meaningless as trying to ban the teaching of higher mathematics. In the opinion of Fischer and many other specialists, the training given to Iranian specialists in Moscow was – and is – aimed at giving them greater knowledge in the area of nuclear security; it has nothing to do with building the nuclear bomb. See: David Fischer, "Pochemu ya podderzhivayu rossiysko-iranskiy kontrakt. Otvet professoru Yablokovu [Why I Support the Russian–Iranian Contract. A Response to Prof. Yablokov]," *Yaderny Kontrol*, No. 6 (June 1995), p. 21, http://pircenter.org/media/content/files/9/13464103580.pdf.

[4] Reviewer's comment, email correspondence with the authors, September 17, 2013.

[5] International Institute for Strategic Studies, *Nuclear Black Markets: Pakistan, A. Q. Khan and the Rise of Proliferation Networks – A Net Assessment* (London: IISS, 2007), p. 70, www.iiss.org/en/publications/strategic%20dossiers/issues/nuclear-black-markets–pakistan–a-q–khan-and-the-rise-of-proliferation-networks—a-net-assessmen-23e1.

Chemical Machinery Research Institute (NIIKhimMash), based in Sergiev Posad, Moscow Region. The incident was discovered thanks to the work of inspectors who were looking for weapons of mass destruction in Iraq. On December 9, 1995, a group of scuba divers hired by the UN Special Commission for Iraq found six missile technology devices at the bottom of the Tigris River, not far from Baghdad. They included the L24-560-4 two-stage gyro-blocks (serial numbers A17373 and Z17530); the L20-17G gyroscopic integrators (serial numbers E17248 and T17215); the LVR-014 air pressure regulator (number LD2.573.014); and a compact engine (serial number A093). The serial numbers betrayed the Russian origin of the gyroscopes.

The incident was discussed in great detail in PIR Center publications, which pointed out that the delivery of gyroscopes from Russia to Iraq was done in such a way as to avoid any observable violations of Russian export-control legislation.[6] Some 800 gyroscopes were sold to a shell company that was set up especially for that purpose in Russia; another 10 gyroscopes had earlier been shipped to Iraq as a sample batch. Formally, Russia's NIIKhimMash was not involved in an export operation; the deal involved one Russian company selling its products to another Russian company, so the contract did not fall under any export-control requirements. There were concerns over the fact that the Russian customs service had failed to spot such a large batch of hardware that could potentially be used for building WMD delivery systems. An even greater cause for concern was that a state-owned Russian company had agreed to such a dubious deal in an effort to resolve its financial difficulties brought on by the break-up of the Soviet Union. Clearly, the company's executives could not plead ignorance about the uses its products could be put to. The company gave the first ten gyroscopes free of charge to Viam Garbiyeh, a Jordanian citizen, who was able to smuggle them out of Russia on a regular flight without any problems with customs. He then brought them to Iraq so that its leadership could decide whether to buy more.[7] Russia was also suspected of exporting engines made by the Votkinsk Plant (republic of Udmurtiya), which were allegedly used in the Iraqi program to transform the Soviet SA-2 surface-to-air missile into

[6] See: Vladimir Orlov and Anna Otkina, "Uroki dela o giroskopakh [Lessons of the Gyroscopes Affair]," *Yaderny Kontrol*, no. 2 (38) (March/April 1998), p. 5, http://pircenter.org/media/content/files/9/13463987270.pdf.

[7] See: Orlov and Otkina, "Uroki dela o giroskopakh," p. 5. See also Vladimir Orlov and William C. Potter, "The Mystery of the Sunken Gyros," *The Bulletin of the Atomic Scientists*, vol. 54, no. 6 (November/December 1998), pp. 34–39.

a medium-range surface-to-surface missile that could be used as a delivery system for biological weapons. Unlike the gyroscope affair, there were no documents to prove the deliveries – but there was no persuasive evidence to the contrary, either. Nevertheless, this case is frequently mentioned in specialist sources, demonstrating that in the 1990s Russia acquired an unwelcome reputation as a country constantly suspected of allowing leaks of various technologies related to WMD and delivery systems.

The imperfections of the Russian export-control system were also recognized in Russia itself. For example, in the 1990s Russian customs officials said that even with regard to radioactive materials they had very few instruments at their disposal to identify and intercept contraband.[8]

Later during the 1990s, the United States sanctioned several Russian institutes and facilities for specific transactions involving transfers of WMD-relevant technology to Iran. In January 1999, for example, the United States sanctioned the Design Institute of Power Technology (known as NIKIET) for making such transfers.[9] NIKIET was sanctioned for transferring graphite reactor technology to Iran. (North Korea, it may be noted, used such a reactor to produce plutonium for nuclear weapons.) The Russian government, however, denied these allegations.[10] The United States lifted the sanctions against NIKIET in March 2004.[11]

Some experts have raised questions as to whether Iran (as well as other countries suspected of harboring nuclear weapons ambitions) succeeded in recruiting Soviet nuclear specialists after the break-up of the Soviet

[8] Kravchenko Nikolay, "Lish' 25 protsentov punktov propuska na granitse oborudovany spetsialnymi priborami dl'a presecheniya kontrabandy [Only a Quarter of Border Control Stations are Equipped with Anti-Smuggling Hardware]," *Yaderny Kontrol*, no. 20–21 (August/September 1996), pp. 8–10; Cherepanov Nikolay, "Customs Service Lacks Effective Controls Over Radioactive Materials," *Yadreny Kontrol*, no. 32–33 (August/September 1997), pp. 29–30.

[9] US Department of State, Bureau of Nonproliferation, Public Notice, "Lifting of Nonproliferation Measures Against Four Russian Entities, Public Notice 4677," *Federal Register* 69, no. 63 (April 1, 2004): 17262. http://www.federalregister.com/Browse/Document/usa/na/fr/2004/4/1/04-7341; Federation of American Scientists, State Department Daily Press Briefing, "Concern over Deterioration in Russian Missile, Nuclear Export Controls," January 13, 1999, www.fas.org/news/russia/1999/990113db-2.htm. See also, Howard Diamond, "U.S. Sanctions Russian Entities for Iranian Dealings," *Arms Control Today*, January 1, 1999, www.armscontrol.org/print/445.

[10] Reviewer's comment, email correspondence with the authors, September 17, 2013.

[11] US Department of State, Bureau of Nonproliferation, Public Notice, "Lifting of Nonproliferation Measures Against Four Russian Entities, Public Notice 4677," *Federal Register* 69, no. 63 (April 1, 2004): 17262. http://www.federalregister.com/Browse/Document/usa/na/fr/2004/4/1/04-7341.

Union.[12] It is difficult to answer those questions with certainty. However, it is fairly safe to assert that Russia has largely succeeded in preventing a nuclear brain drain; some of the credit for that must go to the intergovernmental project called the International Science and Technology Center (ISTC), which helped former Soviet weapon scientists find research opportunities that used their skills on non-military projects.

Indeed, despite the real risks of Russian nuclear specialists leaving to work in other countries, few, if any, appear to have actually done so because Russian specialists have mostly behaved responsibly and declined job offers from countries suspected of nuclear proliferation.[13] At the same time, we should take into account more skeptical views regarding a possible brain drain from Russia to rogue states. For example, according to media, in 1992 the Russian Federal Security Service (FSB) intercepted a charter plane scheduled to carry missile designers bound for North Korea. There were also a number of contradictory reports indicating that a few Russian scientists may have traveled to Iran. No cases of Russian nuclear scientist participation in the Iranian nuclear program have been publicly confirmed, however.

Some Western experts believe that the Russian scientist Vyacheslav Danilenko is an indisputable example of a Russian nuclear weapons specialist providing such assistance. Danilenko worked for several decades in the Russian nuclear weapon complex Chelyabinsk-70 (although he now lives in Ukraine). In 2011 the *Washington Post* published an article alleging that he provided expertise in the development of nuclear detonators for Iran while he was working at the Iranian Physics Research Center between 1996 and 2002, a period, it is now known, of intensive Iranian work on its clandestine nuclear program, including nuclear weapon detonator research and construction of the Natanz uranium-enrichment plant, which was exposed in August 2002.[14] Danilenko has denied these accusations. In November 2011,

[12] Yablokov, "Nekotorye voprosy po povodu atomnoi sdelki s Iranom," p. 20.

[13] Sergey Vorobiov, First Deputy Executive Director (2007–12), International Science and Technology Center (ISTC), interview with the authors, Moscow, March 30, 2012.

[14] Joby Warrick, "Russian Scientist Vyacheslav Danilenko's Aid to Iran Offers Peek at Nuclear Program," *Washington Post*, November 13, 2011, www.washingtonpost.com/world/national-security/russian-scientist-vyacheslav-danilenkos-aid-to-iran-offers-peek-at-nuclear-program/2011/11/12/gIQAeuiCJN_story.html; International Atomic Energy Agency, *Implementation of the NPT Safeguards Agreement and relevant Provisions of Security Council Resolutions in the Islamic Republic of Iran*, GOV/2011/65, November 8, 2011, Annex.

the IAEA published a periodic report on the Iranian nuclear program apparently referring to Danilenko, stating:

> The Agency has strong indications that the development by Iran of the high explosives initiation system, and its development of the high speed diagnostic configuration used to monitor related experiments, were assisted by the work of a foreign expert who was not only knowledgeable in these technologies, but who, a Member State has informed the Agency, worked for much of his career with this technology in the nuclear weapon programme of the country of his origin. The Agency has reviewed publications by this foreign expert and has met with him. The Agency has been able to verify through three separate routes, including the expert himself, that this person was in Iran from about 1996 to about 2002, ostensibly to assist Iran in the development of a facility and techniques for making ultra-dispersed diamonds ("UDDs" or "nanodiamonds"), where he also lectured on explosion physics and its applications.[15]

It should be clarified that Danilenko is not an expert in nuclear physics, and some have strong doubts about whether he could really have become the "father of Iran's nuclear bomb" as the Western media sometimes argues.[16] In the end, despite the implicit accusations in the IAEA report, the matter remains a subject of significant speculation.

Whatever the facts in the Danilenko case, broader efforts by the ISTC to engage weapons scientists in civilian projects, as well as the Russian government's ability to provide adequate financing for Russian research programs, have helped to prevent a nuclear brain drain to rogue states.

Some historical aspects of the nuclear cooperation between Iran and Russia still remain unknown because Iran has declined to provide to the IAEA full required information on its past nuclear activities. Historical experience demonstrates that countries with developed nuclear infrastructure (like Sweden or Switzerland) clarified the military aspects of their nuclear programs only decades later after ending attempts to obtain nuclear weapons. The December 2015 IAEA report on Iranian past

[15] International Atomic Energy Agency, GOV/2011/65, November 8, 2011, Annex, paragraph 45. Regarding the identification of the expert referred to by the IAEA report as Danilenko, see David Albright, Paul Brannan, Mark Gorwitz, and Andrea Stricker, "ISIS Analysis of IAEA Iran Safeguards Report: Part II - Iran's Work and Foreign Assistance on a Multipoint Initiation System for a Nuclear Weapon" (Washington, D.C.: Institute for Science and International Security, November 13, 2011), http://isis-online.org/isis-reports/detail/irans-work-and-foreign-assistance-on-a-multipoint-initiation-system-for-a-n/.

[16] Victor Vasiliev, "Vyacheslav Danilenko: otets iranskoy yadernoy bomby? [Vyacheslav Danilenko: Father of Iran's nuclear bomb?]," *Voice of America*, November 14, 2011, www.golos-ameriki.ru/content/iran-nuclear-program-2011-11-14-133831888/248416.html.

nuclear activities, prepared in accordance with the Joint Comprehensive Plan of Action (JCPOA) between the P5+1 countries and Iran, was, in our view, a reasonable compromise. No "Russian connection" from the past years was revealed in the document.

In 2006, the Russian government issued a White Paper on Nonproliferation, which stated that over the previous several years authorities had conducted over sixty criminal investigations into cases of unauthorized exports of controlled products.[17] The White Paper also said that Russian security agencies had identified and taken measures against more than thirty foreign citizens and companies doing business in Russia who tried to buy and smuggle out of the country various products and technologies that could be used to create WMD or delivery systems.

The White Paper does not list all of these criminal cases – but it does name several individuals and organizations caught trying to steal technologies.[18] On the one hand, this information demonstrates that there has been genuine demand on the black market for Russian WMD-related technologies, including nuclear weapons technologies, and that there is, indeed, a risk of proliferation. On the other hand, the White Paper insists that all the attempts to smuggle these technologies out of Russia were thwarted, suggesting that the country is well able to prevent such leaks.[19]

[17] Permanent Mission of the Russian Federation to the International Organizations in Vienna, *Rossiyskaya Federatsiya i situatsiya v oblasti nerasprostraneniya oruzhiya massovogo unichtozheniya i sredstv ego dostavki: ugrozy, otsenki, zadachi i puti ikh realizatsiyi [The Russian Federation and Nonproliferation of Weapons of Mass Destruction and Delivery Systems: Threats, Assessments, Problems and Solutions]*, December 31, 2005; http://rusmission.org/7/1/111.

[18] Individuals named in the report include:

- US citizen Nader Modanlo, President of Final Analysis, Inc., who was refused entry to the Russian Federation for attempting to circumvent Russian export control legislation in order to acquire technical documentation on missiles and satellites for subsequent transfer to Iran;
- Pakistani citizen Muhammad Aslam, who was refused entry to the Russian Federation for using his position as an employee of the Tabani Corporation's Moscow office to conceal efforts to acquire Russian weapons, strategic materials, and dual-use goods for the Pakistani missile and nuclear programs;
- Iran's Sanam Industrial Group which was foiled in its attempt to place an order with Trud Science and Production Association for the fabrication of missile engine components under the guise of gas-pumping equipment. The Sanam Group's activities in the Russian Federation have been suspended. See: "The Russian Federation and Nonproliferation of Weapons of Mass Destruction and Delivery Systems: Threats, Assessments, Problems and Solutions," CNS Translation.

[19] Some experts voiced their disagreement with certain aspects of the 2006 assessment of the Russian officials. For example, Nikolay Sokov, writing later that year, believed that the information contained in the document had a clear political subtext. He argued that "all examples involving illicit exports were intended for the Iranian and the Pakistani nuclear

It must be admitted that there is simply not enough information about nuclear technology leaks from Russia. The only authoritative source, the government's 2006 White Paper, mentions only a few individual cases; most of the other incidents have not been disclosed for political or other reasons – one of those reasons being Russia's traditional secrecy on all matters relating to its nuclear weapons program. It is quite telling that the 2006 White Paper was the first detailed and comprehensive document of that nature released into the public domain. Up until that point, all such documents remained strictly classified.[20] The Russian addiction to secrecy is also the likely reason why, as of late 2015, there has not been another White Paper on nonproliferation since the 2006 publication. Thus, this analysis of the potential risks of nuclear technology leaks from Russia, both in the past and in the present, relies on known cases of missile technology and equipment leaks, as well as smuggling of conventional weaponry out of Russia.

To summarize, the reasons Russia was suspected of allowing sensitive technology leaks in the 1990s were as follows:

1. Shortcomings of the Russian export-control system in the 1990s, caused primarily by gaps in the legislation and regulation, as well as lack of the necessary technology (i.e. radiation detectors).
2. A misplaced emphasis in assessing the threat of nuclear technology leaks. There is no denying that the risks were real – but Western experts and politicians often failed to understand what the main source of those risks was. They overestimated the dangers posed by proliferation from Russia, and underestimated the much more serious proliferation risks posed by countries such as Pakistan. This failing is recognized by Robert Einhorn, a reputable US expert and former senior official. In a book by journalist Gordon Corera, he is quoted as saying that "Pakistan was not on our radar screen... It was our assumption that... Pakistan–Iranian nuclear cooperation was not a significant factor."[21]

and missile programs. The perpetrators in these cases were US, Pakistani, and Iranian citizens and companies. Interestingly, the White Paper is silent about attempted exports to China, even though there have been numerous recent cases involving alleged attempts to transfer sensitive technologies and equipment from Russia to China." Nikolai Sokov, "Russian's White Paper on WMD Nonproliferation," *CNS*, July 25 2006, www.nonproliferation.org/russians-white-paper-on-weapons-of-mass-destruction-nonproliferation/.

[20] Sokov, "Russian's White Paper on WMD Nonproliferation."

[21] Gordon Corera, *Shopping for Bombs: Nuclear Proliferation, Global Insecurity, and the Rise and Fall of the A. Q. Khan Network* (New York and Oxford: Oxford University Press: 2006), p. 79. Commenting on that admission, one of the authors of this paper had this to say in another article: "Many in Russia well remember how much effort Einhorn

To summarize the background section of this chapter, it must be said that Western countries tended to exaggerate the risks of nuclear material and technology leaks from Russia. Nevertheless, those risks were real, and the Russian leadership was well aware of them. To address the situation, Russian leaders have taken a number of measures with regard to legislation and technology provision.

RUSSIAN LEADERSHIP'S MEASURES TO REDUCE THE RISK OF NUCLEAR TECHNOLOGY LEAKS FROM RUSSIA

It is clear from the previous section of this chapter that the situation with sensitive technology leaks from Russia in the 1990s and early 2000s was worrying, though not catastrophic. That is why the Russian government had to undertake a number of steps to improve its laws and regulations dealing with nuclear materials and technologies, especially in the area of technology export control. This section offers a review of the key Russian laws and regulations aimed at combating the black market for nuclear technologies, and looks at the current state of their implementation.

The current Russian export-control system was taking shape in the 1990s and 2000s. The structure of that system is outlined in Figure 1.

As Figure 11.1 demonstrates, the Russian export-control system is regulated by several agencies. The agency most directly involved in this area is the Federal Service for Technical and Export Control (FSTEC), which is currently subordinated to the Ministry of Defense. The government is now considering a proposal to subordinate the agency directly to the Cabinet.[22] The governmental Export Control Commission coordinates the work of several other agencies involved in export control.

The Russian export-control system is based on several laws and regulations. Its general outlines are reflected in such basic documents as the Russian Foreign Policy Concept; the Principles of State Policy on the Nonproliferation of WMD and Delivery Systems; and the Principles of State Policy on Chemical and Biological Security to 2010 and Beyond.

had spent trying to prevent any meaningful contacts between Russian companies and Iran if there was even a purely theoretical possibility of those contacts helping the Iranian nuclear program." See Vladimir Orlov, "Khan Networks: Eyes Wide Shut," *Security Index*, no. 3 (85) (Autumn 2008), p. 154.

[22] "Minoborony pytayutsa podsokratit' eshche na odnu federal'nuyu sluzhbu [MoD Trying to Cut Another Federal Service]," *Kommersant Newspaper*, April 4, 2013, http://kommersant.ru/doc/2161864.

FIGURE 11.1: The Russian Export Control System
Source: Vladislav Malkevich. *Export Control: From Confrontation to Cooperation, Moscow* (in Russian), 2012

More specific measures to combat the black market for nuclear technologies are spelled out in the documents listed in Figure 11.2. These documents directly regulate practical efforts in this area. Another important document, which has already been mentioned, was adopted in 2006 and approved by the president. Its official title is "The Russian Federation and Nonproliferation of Weapons of Mass Destruction and Delivery Systems: Threats, Assessments, Problems and Solutions;"[23] the document is informally referred to as the Russian White Paper on Nonproliferation. Unlike the documents listed in Figure 11.2, the White Paper does not contain any specific prescriptions or guidelines. However, it is important as an in-depth review by government experts of the current situation, including the state of affairs with nuclear technology leaks. The White Paper reflects the official Russian stance on the situation with the nuclear black market both within Russia and internationally.

Let us now look at the specific documents that aim to counter the nuclear black market. Of the documents listed in Figure 11.2, the most important piece of legislation is the law "On Export Control," which was adopted on July 18, 1999 (the latest edition is from February 6, 2011). Another key document is the Customs Code of 2003, which regulates the

[23] Permanent Mission of the Russian Federation to the International Organizations in Vienna, *Rossiyskaya Federatsiya i situatsiya v oblasti.*

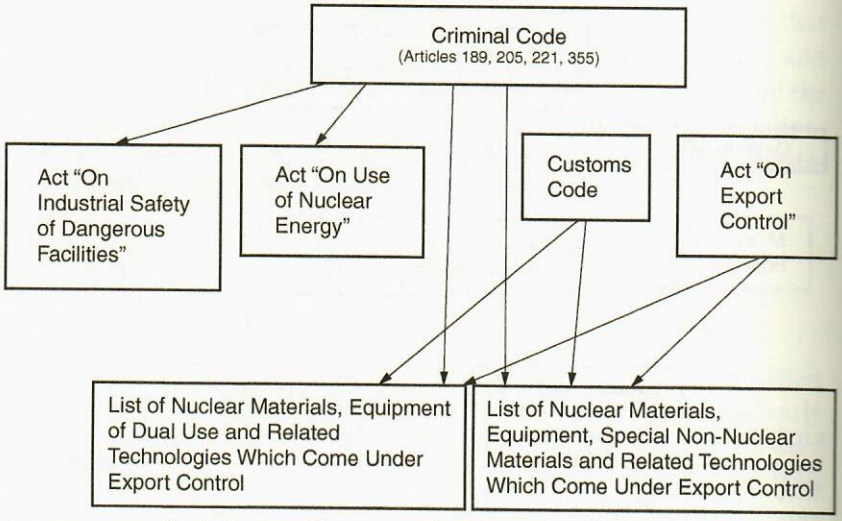


FIGURE 11.2: Basic Russian Documents for Preventing Nuclear Technology Proliferation

treatment of nuclear material and technology exports by the Russian customs service. The laws "On the Use of Nuclear Energy" of November 21, 1995 (updated November 11, 2003) and "On Industrial Safety at High-Risk Facilities" of July 21, 1997 (updated January 10, 2003) have some limited relevance for the first and second line of defense of nuclear technologies. The issue is dealt with more directly in the export-control lists for materials and technologies. Russia has six different control lists, of which two deal with nuclear materials and technologies. The first of them, listing "Nuclear Materials, Equipment, Special Non-nuclear Materials and Relevant Technologies Subject to Export Control,"[24] was approved by a presidential decree on February 14, 1996. It has undergone several revisions over the years; the latest revision was approved by a presidential decree on September 1, 2014. The second control list was approved by Presidential Decree No. 36 of January 14, 2003, "On Approving the List of Dual-Use Equipment and Materials and Relevant

[24] "Ob utverzhdeniyi spiska yadernykh materialov, oborudovaniya, spetsialnykh neyadernykh materialov I sootvetstvuyushchikh tekhnologiy, podpadayushchikh pod eksportny kontrol [On Approving the List of Nuclear Materials, Equipment, Special Non-nuclear Materials and Related Technologies Subject to Export Controls]," Presidential Decree No. 202 of February 14, 1996. Text of the decree as of November 2017, http://fstec.ru/eksportnyj-kontrol/zakonodatelstvo/98-ukazy/324-ukazprezidentarossijskoj-federatsii-ot-14-fevralya-1996-g-n-202.

Nuclear-Used Technologies, Subject to Export Control" (revised September 1, 2014).[25]

These lists determine which nuclear materials and technologies are subject to export control and require special export procedures. These materials and technologies can be exported only to those countries that are not in breach of the international nuclear nonproliferation regime.

Figure 11.2 also demonstrates that Russia has criminalized all operations on the black market for nuclear materials and technologies. Articles 189, 205, 221, and 355 of the Russian Penal Code outline criminal responsibility for violations of export-control legislation, etc.

Another thing to take into account is that the Russian export-control legislation is quite different from similar legislation in other countries; experts believe that the differences are not in Russia's favor.[26] They say that the Russian export-control system is too bureaucratic because too many government agencies are involved. In addition, there are six different lists of products subject to export control; in the European Union, for example, there is only one such list. The presence of six different lists, of which not one but two contain nuclear materials and technologies, significantly complicates the export-control procedures.

Nevertheless, and despite the imperfections and unnecessary complexity of the Russian export-control system, experts tend to agree that the system has become quite effective by now.[27] Its practical implementation is best analyzed using the example of specific Russian companies involved in exports of nuclear or other radioactive materials and technologies.

[25] "Ob utverzhdeniyi spiska oborudovaniya i materialov dvoinogo naznacheniua i sootvetstvuyushchikh tekhnologiy, primenyamykh v yadernykh tselyakh, v otnosheniyi kotorykh osushchestvlyayetsa eksportny control," [On Approving the List of Dual-Use Equipment and Materials and Relevant Nuclear-Used Technologies, Subject to Export Control] Presidential Decree No. 36 of January 14, 2008, (last revision October 14, 2008), http://fstec.ru/eksportnyj-kontrol/zakonodatelstvo/98-ukazy/325-ukaz-prezidenta-rossijskoj-federatsii-ot-14-yanvarya-2003-g-n-36.

[26] Vladislav Malkevich, "Eksportny kontrol': ot protivostoyaniya k sotrudnichestvu [Export Control: From Confrontation to Cooperation]" (Moscow: Society for the Preservation of Literary Heritage, 2012), p. 315.

[27] Elina Kirichenko, statement at the first meeting of the Working Group under the PIR Center Advisory Board on the Prospects of Russian Participation in International Cooperation on Nonproliferation and Nuclear Security. See: PIR Press, "Nuclear Security After Nunn-Lugar Program," April 1, 2013, http://pircenter.org/en/news/6426-nuclear-security-after-nunnlugar-program.

INTERNAL COMPLIANCE PROGRAMS IN RUSSIA AS AN INSTRUMENT AGAINST THE BLACK MARKET FOR NUCLEAR TECHNOLOGIES

Internal Compliance Programs: Legislation and Regulation

Governments traditionally play an important role in ensuring the effectiveness and reliability of the national export-control systems, and Russia is no exception. However, it is physically difficult for government agencies to monitor the vast flow of foreign trade in numerous products and technologies that can be used for making nuclear weapons. In addition, amid the ongoing globalization trends excessive government controls over exports stifle economic growth.

That is why internal compliance programs are becoming increasingly important. Article 16 of the 1999 law "On Export Controls" introduces the definition of internal compliance programs in companies and organizations. In accordance with that definition, an internal compliance program (ICP) is a collection of organizational, administrative, information-related, and other measures undertaken by organizations in order to comply with export-control rules.[28] The FSTEC website contains detailed explanations of all these measures, which include:

- First, organizational measures: corporate procedures and regulations for employees conducting negotiations and signing and implementing foreign trade contracts to ensure compliance with export control legislation (order, corporate standard, instruction, etc).
- Second, administrative measures: establishing penalties in accordance with Russian labor, administrative, civil, and criminal legislation for violating the corporate procedures for foreign trade operations.
- Third, information measures: setting out procedures that regulate information exchange with government agencies on export control issues, establishing the responsibilities of employees with regard to keeping up to date the organization's information about current export

[28] Law No. 183-FZ of July 18, 1999 "On Export Control" (revisions No. 196-FZ of December 30, 2001; No. 58-FZ of June 29, 2004; No. 90-FZ of July 18, 2005; No. 283-FZ of November 29, 2007; No. 318-FZ of December 1, 2007; No. 89-FZ of May 7, 2009; No. 169-FZ of July 1, 2011; No. 242-FZ of July 18, 2011; and No. 409-FZ of December 6, 2011), http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=122943.

control rules and regulations, and staff training in the area of export control.[29]

The government benefits from ICP systems because they reduce the need for government agencies to verify whether the export-destined products are on the control lists, which is a laborious process. Much of the work involved is done by the companies themselves. It is these companies, and not the treasury, who bear the costs of these procedures. In the end, it is simpler and less time-consuming for the company itself to cross-check its products against export-control lists than for the government to conduct the same cross-checks for hundreds of thousands of individual companies. As a result, ICP systems produce savings for the treasury, and enable companies to minimize costly delays with exports.

This is why the law "On Export Control" contains a recommendation for all Russian companies to establish an ICP system. For most companies the undertaking is voluntary, but the law clearly specifies the kind of firms for which such a system is mandatory. This mandatory requirement applies to companies and organizations that pursue research and production activities related to the provision of Russian defense and national security capabilities, and which regularly receive revenues from export and import operations with controlled products and technologies.[30]

ICP systems offer obvious economic benefits – but at the same time, they also pose certain proliferation risks. With such systems, the government essentially delegates a large part of export-control responsibilities to commercial entities, which by their very nature dislike any forms of export controls or restrictions because they want to maximize their profits.

Russia has resolved this problem of confidence by introducing a thorough procedure for all companies that wish to obtain the privileges associated with having an internal compliance program system.

To begin with, simply establishing an ICP system is not enough for a company to obtain the privileges (i.e., having a general export license and submitting its own assessments of whether the exported products fall under any export-control lists). To qualify for these privileges, each company must first demonstrate to the government that its ICP system is effective.

[29] Federal Service for Technical and Export Control, "Internal Compliance Program. Creating Internal Compliance Program Systems," FSTEC website, January 9, 2013, http://fstec.ru/vnutrifirmennye-programmy-ek/92-deyatelnost/tekushchaya/eksportnyj-kontrol/vnutrifirmennye-programmy/293-vnutrifirmennaya-programma.

[30] Law No. 183-FZ of July 18, 1999 "On Export Control," http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=122943.

The government's recognition of such a system's effectiveness comes in the form of state accreditation issued to companies by the authorized body, the FSTEC.[31] In simple terms, government accreditation is a certificate of confidence in the individual company's ICP arrangements.

The companies and organizations that have successfully passed accreditation receive a certificate which is usually valid for a three-year term, and which can be extended using the same procedure. All organizations that have received government accreditation must submit a brief annual report to the FSTEC by March 1 of each year.[32]

Russian laws do not stipulate any pre-determined requirements to the precise structure and organization of internal compliance programs. The law "On Export Control" has introduced a mandatory requirement for some kinds of companies to put in place an ICP system – but it does not specify what exactly that system should look like. Clearly, a degree of freedom given to companies in determining their own ICP arrangements does not release the government from its responsibility to make sure that these arrangements are effective. That is why Russia has a tried and tested accreditation procedure, whereby companies must continuously demonstrate to the government that their ICP arrangements are effective and reliable.

Assessing the Risks of Nuclear Technology Leaks from Russian Companies

Russia has a large number of companies and organizations that could potentially be a source of proliferation of nuclear and other radioactive materials, as well as related technologies. We tried to assess the risks of nuclear technology leaks from Russian companies and organizations by analyzing the information available at the official websites of the Russian nuclear industry companies and conducting interviews with representatives of several companies.

[31] "Procedure for Government Accreditation of Organizations That Have Established Internal Compliance Program," approved by Cabinet Resolution of February 29, 2000 No. 176 (latest revision July 21, 2008).

[32] The report must contain the following information: (a) size and structure of exports; (b) organizational and personnel changes pertaining to foreign trade operations; (c) information about the company executive in charge of export control; (d) information about export control training events for employees. See: Federal Service for Technical and Export Control, "Internal Compliance Program. Creating Internal Compliance Program Systems."

First of all, it is important to analyze the export-control policies of Russian companies such as JSC "Techsnabexport" (brand name TENEX), which is the world's largest exporter of products and services of the Russian nuclear fuel cycle, with a substantial share in the industry's total foreign-trade turnover.[33] The company unites a number of the Russian facilities that could potentially become sources of nuclear technology leaks.

JSC "Techsnabexport" was one of the first Russian companies to establish an ICP. The main objectives of the JSC "Techsnabexport" internal compliance program include preventing transfer to foreign individuals of scientific and technical information that could incur damage to the national interests of the Russian Federation and creating a mechanism of inspections to ensure the legitimate character of foreign trade transactions. The export-control system has been operational in JSC "Techsnabexport" since 2001. It allows monitoring foreign trade operations with the following foreign trade objects:

- nuclear materials, equipment, special non-nuclear materials, and relevant technologies;
- equipment, dual-purpose materials, and relevant technologies used for nuclear purposes.[34]

A Certificate of Accreditation # 002 issued by the FSTEC confirms the efficiency of ICP in the JSC "Techsnabexport." The certificate allows the JSC "Techsnabexport" to obtain general licenses for deliveries of controlled goods, equipment, and technologies. According to the official website of "Techsnabexport," the state provides to the company the right to obtain the licenses, which means another level of responsibility and a degree of freedom in the practical implementation of foreign trade activities to the organizations determined to have an unblemished "export-control history," and the JSC "Techsnabexport"(according to its website) is no doubt one such organization.[35]

The Siberian Chemical Combine (SCC) is another Russian company that could hypothetically become a source of proliferation of sensitive nuclear technologies. This is the only working facility in the world that has the capability to process uranium in any shape or chemical form. It is

[33] TENEX, "Company Profile," JSC "Techsnabexport," www.tenex.ru/wps/wcm/connect/tenex/site.eng/company/.
[34] TENEX, "Company Profile," JSC "Techsnabexport."
[35] TENEX, "Company Profile," JSC "Techsnabexport."

also one of the largest global suppliers of uranium used in the production of nuclear fuel. In addition, the SCC is part of the Russian nuclear weapons industry.[36] According to the SCC's own documents, the company has implemented a number of export-control measures that aim, among other things, to reduce the risk of nuclear technology proliferation. These measures include, first and foremost, improving the nuclear security culture and responsibility among the personnel that possess sensitive expertise.[37]

Other Russian nuclear industry companies that could potentially be sources of nuclear technology proliferation include the Urals Electrochemical Combine; the Angarsk Electrolysis Chemical Combine; the Russian Federal Nuclear Center – All-Russian Science and Research Institute of Experimental Physics (VNIIEF); and several others.

Some of the Russian companies represent a very insignificant risk of nuclear technology proliferation because they are not involved in any exports, or do not use any sensitive technologies. For example, speaking about the risks of nuclear material and technology leaks from the International Uranium Enrichment Center (IUEC), the organization's chief specialist for IAEA safeguards, Aleksandr Panasyuk, told one of the authors of this chapter in an email that until recently the IUEC had not exported any nuclear material. The first delivery of nuclear material from the center was made to a Russian company, which then exported that material to another country. The IUEC is about to commence exports after receiving requests for uranium supplies from its stakeholders.[38]

As for any leaks of proliferation-sensitive nuclear technologies, Panasyuk believes that such an incident can be ruled out as well. First, the intergovernmental agreement on setting up the IUEC, the company's Charter, and other documents ban any transfer of classified technologies not only to third parties but even to the non-Russian IUEC stakeholders. Second, Russia is the founder of the company and owns a 50 percent plus one stake (i.e. holds the controlling stake), which makes any leaks of classified information impossible.[39]

[36] Siberian Chemical Combine, "Mission of the Siberian Chemical Combine," corporate website, www.atomsib.ru/missiya-kombinata.

[37] Siberian Chemical Combine, "Policy of the Siberian Chemical Combine leadership in the area of export controls," Siberian Chemical Combine corporate website.

[38] Aleksandr Panasyuk, chief specialist for IAEA Safeguards, International Uranium Enrichment Center, email correspondence with one of the authors, May 14, 2013.

[39] Panasyuk, email correspondence, May 14, 2013.

It should also be noted that there are no risks of nuclear technologies proliferation from JSC "Isotope," a division of the Rosatom state corporation, because the company does not actually use any proliferation-sensitive technologies.[40]

On the whole, according to estimates by representatives of Russian nuclear industry companies, the ICP systems of these companies are effective, and the risk of proliferation of sensitive technologies has essentially been reduced virtually to zero. It has to be said, however, that some Western analysts do not share such an optimistic point of view. The focus of their more negative assessment, however, is not on "nuclear-specific" items of the type produced by the Russian nuclear industrial concerns noted above and other elements of that industry, but rather on dual-use items produced by numerous commercial concerns throughout the Russian economy. For example, a periodic report to the US Congress prepared by the US Director of National Intelligence, the *Unclassified Report to Congress on the Acquisition of Technology Relating to Weapons of Mass Destruction and Advanced Conventional Munitions, Covering 1 January to 31 December 2011*, noted that "North Korea and entities in Russia and China continue to sell technologies and components in the Middle East and South Asia that are dual-use and could support WMD and missile programs."[41]

At the same time, the report did not specify which Russian companies were sources of proliferation of sensitive nuclear technologies, nor has the United States sanctioned any Russian firms because of proliferation concerns for many years. In addition, the authors of the report recognize officially approved Russian–Iranian nuclear industry cooperation is within the IAEA safeguards system and do not note any concerns regarding officially approved Russian–Indian and Russian–Chinese nuclear trade. In other words, claims made by the authors of the report and by other Western analysts to the effect that Russian nuclear industry companies are sources of nuclear technology proliferation to threshold countries deserve to be noted, but have not been backed by any specific, well-documented examples, leaving their overall significance very much in doubt.

[40] Igor Makarevich, acting head of the nuclear and radiation safety and security department at JSC Izotop, email correspondence with one of the authors, May 16, 2013.

[41] US Director of National Intelligence, *Unclassified Report to Congress on the Acquisition of Technology Relating to Weapons of Mass Destruction and Advanced Conventional Munitions, Covering 1 January to 31 December 2011*, www.fas.org/irp/threat/wmd-acq2011.pdf.

Of course, certain risks of sensitive technology proliferation from Russian nuclear industry companies still exist. This was recognized by Aleksandr Loktev, head of the Rosatom internal compliance and audit department. Specifically, Mr. Loktev cited some examples of corruption-related irregularities at nuclear industry companies uncovered during audits. He spoke, in particular, of

> large deals being signed without the vetting of the [Rosatom] state corporation, which creates fertile ground for irregularities. They are sometimes trying to trick us by misrepresenting a large deal as several smaller ones in the documents ... Such cases were uncovered and put an end to during an audit at FGUP NPO Khlopin Institute of Radium. The head of one of the company's branches signed numerous contracts with front companies that were not economically active and were registered to figurehead owners.[42]

This particular violation was committed purely for money-laundering purposes, so naturally the official Rosatom representative made no direct mention in his statement of any specific instances of nuclear technology proliferation resulting from corruption.

However, the example demonstrates the theoretical possibility of a large deal being misrepresented as several smaller ones in order to facilitate illegal sales of sensitive nuclear technologies. Nevertheless, Rosatom is taking energetic steps to eliminate any theoretical possibility of proliferation. For example, every two years the corporation adopts and consistently implements the aforementioned comprehensive programs of countering theft in the nuclear industry. These programs appear to be effective, as demonstrated by the absence of any proven cases of nuclear technology proliferation from Russian nuclear industry companies.

On the whole, there have not been any documented cases of nuclear technology leaks in recent years. Thus, for the moment, the risk of such leaks remains more hypothetical than real.

RISKS OF POTENTIAL NUCLEAR TECHNOLOGY LEAKS FROM RUSSIAN EDUCATIONAL INSTITUTIONS

Educational institutions, where nuclear physics is taught, could also be a source of sensitive nuclear technology leaks. In Russia there are a number of such educational institutions. The situation with potential nuclear

[42] Aleksandr Loktev, "Rosatom vnedryaet sistemy obshchestvennogo kontrol'a" [Rosatom Implements a Public Control System]," April 23, 2010; Russian Atomic Community, www.atomic-energy.ru/interviews/2010/04/23/10626.

technology leaks from MEPhI National Nuclear Research University – Russia's premier nuclear engineering school – was discussed in an interview with Viktor Murogov, who is a professor at MEPhI. Murogov told one of the authors that MEPhI University has an internal compliance program. Before MEPhI publishes any research paper, the university's export commission convenes to discuss whether such a paper can be published in open sources. The commission designates some papers as suitable for internal use only; the information can also be supplied directly to the relevant Russian bodies and agencies. In other words, all technologies developed at MEPhI must pass internal vetting before they are allowed to circulate beyond Russia.[43]

Professor Murogov has expressed a certain degree of skepticism about MEPhI University's internal compliance program. He says he does not doubt the professionalism and good intentions of the professors who are responsible for that program. However, he believes there is a problem caused by the lack of any clear criteria for deciding which nuclear technologies can be passed on to foreigners, and which are too sensitive for export.[44] For example, some specialists believe that it is possible to teach all nuclear technologies, except those specifically relevant to nuclear weapons, to students from third countries where nuclear energy industry development is in the early phases. Others insist, however, that such an approach poses serious risks for the nonproliferation regime. They say that if only bomb-related knowledge is declared off-limits, third countries might still be able to obtain other sensitive know-how – such as nuclear fuel-cycle technologies – which can be used to develop nuclear weapons. In the past, the Soviet Union supplied finished nuclear reactors to third countries, and trained local specialists only in the operation of those reactors. As a result, those specialists did not receive any sensitive knowledge about reactor design. That made sure that they would not be able to use indigenously designed reactors to develop nuclear weapons. Many experts continue to believe that such an approach would be best for the nonproliferation regime.

Several attempts have been made in Russia to come up with a precise classification of nuclear knowledge in terms of the suitability of that knowledge for teaching to foreigners. In 2003 President Putin instructed the Ministry of Education to develop a concept of training programs for

[43] Viktor Murogov, professor, MEPhI University, interview with the authors, Moscow, May 14, 2013.

[44] Murogov interview, Moscow, May 14, 2013.

foreign students. Such a concept would drastically reduce the risks of nuclear technology leaks from Russia via foreign students, and strengthen the Russian export-control system. However, due to bureaucratic complications the president's instruction was never fulfilled. In 2008 MEPhI teachers submitted a draft concept of nuclear education to the Education Ministry, but the proposal was rejected, also because of excessive bureaucracy. One of the ministry's officials declared that approval of the concept of nuclear education remained out of the question so long as the general education concept was still in the making.[45] The problem is, the ministry is not actually interested in having these concepts put in place because once they have been approved, additional financing will be needed for their implementation.

Viktor Murogov believes that putting in place a concept for the education of foreign students, including its nuclear component, would require the president's personal intervention: Vladimir Putin should insist that his instruction issued back in 2003 be fulfilled.[46]

In the United States, there are no clear prescriptions or even recommendations as to what kind of knowledge can be taught without undermining the nuclear nonproliferation regime. US universities are not controlled by the government, and they make their own decisions within the parameters of rules on "deemed exports." Nevertheless, Murogov believes that the government in Washington could potentially exert some influence on universities that offer nuclear-related courses by means of various financial instruments.[47]

The position of the United States and other nuclear powers with regard to controlling the spread of nuclear know-how via training courses for foreign students is important for Russia's own export-control system. After all, such a system can only be successful if there is effective international cooperation. All the countries that offer nuclear training must agree upon a common set of criteria for deciding what kind of knowledge is acceptable to teach to foreign students. Such a coordinated approach is indispensible for the success of international efforts to prevent the proliferation of sensitive nuclear technologies. A common set of criteria would prevent unfair competition between the countries that offer nuclear education and training services.

[45] Murogov interview, Moscow, May 14, 2013.
[46] Murogov interview, Moscow, May 14, 2013.
[47] Murogov interview, Moscow, May 14, 2013.

To summarize, there is a potential risk of sensitive nuclear technology leaks from Russian educational institutions because MEPhI nuclear research university is now teaching students from other countries – including Egypt, Jordan, Vietnam, and Bangladesh. According to Murogov, as of this moment, none of these students has actually received any nuclear training; all of them are still learning Russian. However, because Russia still lacks an official concept for educating foreign students, it remains unclear what kind of nuclear knowledge will be taught to these students, and how that knowledge will be categorized in terms of the risks posed for the nonproliferation regime. Murogov believes that any such distinctions should take into account the fact that a lot of sensitive information is already freely available on the Internet.[48] In our opinion, however, this does not necessarily mean that such information is easy to understand, let alone use for practical purposes, without proper training that can only be obtained from education establishments such as MEPhI University. These universities must therefore have a clear policy as to what kind of knowledge is safe to teach.

RUSSIAN STANCE ON THE INTERNATIONAL BLACK MARKET FOR NUCLEAR TECHNOLOGIES AND INTERNATIONAL EFFORTS TO STOP IT

The problem of a nuclear black market remains a concern for Russia, and certain risks of nuclear technology leaks from Russian territory have yet to be eliminated. As we have already mentioned, one of the potential sources of such leaks is MEPhI National Nuclear Research University. The institute itself is not to blame for this; the real reason is the lack of coordinated international norms regulating nuclear education and training. That is why resolving the problem of the black market for nuclear technologies once and for all, in Russia as well as internationally, requires a coordinated international effort in this area.

Cooperation between Russia and the United States is especially important in that regard. The risks of nuclear technology leaks via the education system are also a problem in the United States, although the United States does not have any institutions like MEPhI, with its deep ties to Russia's nuclear weapons complex. However, in the United States, foreign students study alongside American students in physics and nuclear engineering

[48] Murogov interview, Moscow, May 14, 2013.

departments across the country.[49] While everything taught in universities is considered open-source and therefore is technically not classified, some of the information may be sensitive and covered by US export control regulations, especially in graduate level engineering studies. Due to the culture in research and academic institutions in the United States that are very critical of any type of censorship, it would be difficult, if not impossible, to simply "ban" certain topics.[50]

With regard to Russia's stance on world trends in countering the appearance of nuclear technology black markets, the most interesting aspect is the Russian position on sanctions against those who violate export-control mechanisms. As the 2006 White Paper affirms, Russia has always been committed to political and diplomatic means of resolving such problems. In Russia's view, the use of force is a measure of last resort that requires authorization by the UN Security Council.[51]

In an interview by the authors, a representative in the Russian Foreign Ministry was skeptical about sanctions. He believes that sanctions are acceptable only if they are not politically biased, and if the violation has been clearly demonstrated.[52] Russian officials do not reject the use of sanctions as such. However, according to the Foreign Ministry representative, it makes more sense to use sanctions against specific individuals and entities rather than entire countries. Here, too, it is important to avoid any political bias, which the Foreign Ministry believes is evident in cases such as the Magnitsky List.[53] Russia, however, did react strongly after the disclosure of Iran's previously secret Fordow enrichment plant, supporting considerably strengthened sanctions against Tehran at the UN Security Council. It remained reluctant, however, to expand the list of sanctioned entities and individuals. Nor did Russia support making inspection of suspect cargoes going to and from Iran mandatory, preferring the formulation that the Council "call upon" states to undertake such inspections. After signing the nuclear deal with Iran (the Joint Comprehensive Plan of Action) in July 2015, Russia has prioritized a policy of lifting sanctions against Iran. Russian officials and experts do

[49] US Department of Energy official (name withheld by request), interview with PIR Center intern Jennifer Dahnke, Washington, D.C., May 20, 2013.

[50] US Department of Energy official interview, Washington, D.C., May 20, 2013.

[51] Permanent Mission of the Russian Federation to the International Organizations in Vienna, *Rossiyskaya Federatsiya i situatsiya v oblasti.*

[52] Representative of the Russian Foreign Ministry (name withheld by request), interview with one of the authors, Moscow, May 20, 2013.

[53] Representative of the Russian Foreign Ministry interview, Moscow, May 20, 2013.

not agree with the position of Israel, Saudi Arabia, and some conservative members of the US Congress who insist on extending sanctions against Iran despite the significant progress in implementing the JCPOA.

Russia's reaction within the Security Council to North Korea's nuclear tests has been similarly cautious.

Russia does not share the Western view on how to deal with those nations that decline, as a matter of principle, to join international export-control regimes. Moscow has its own solution, which does not rely on the use of force or sanctions. It believes that the international community could deal with countries that are seen as unreliable in terms of export controls by using the Additional Protocol to the IAEA Safeguards agreements. In Russia's opinion, application of the Additional Protocol should be one of the factors taken into account when deciding whether to allow nuclear exports to any specific country,[54] although Moscow declined to apply this criterion in pressing ahead with its sale to Iran of the Bushehr nuclear power plant even after Iran's secret nuclear projects were exposed.

Russian cooperation with the IAEA in fighting the black market for nuclear technologies currently is not very significant.[55] However, Russia participates in various international nuclear projects under IAEA auspices. As one of the founding members of the agency and one of the most advanced nuclear powers, Russia plays an important role in IAEA programs. It pays an annual fee to the agency's budget, and makes financial contributions to technical cooperation and nuclear security funds operated by the IAEA.[56] Russian initiatives to develop innovative nuclear technologies include measures against such technologies being used in weapons programs or traded on the nuclear black market. For example, Russia supports the IAEA international project on innovative nuclear reactors and fuel cycles (the INPRO project). The specialists working on that project have developed a procedure for assessing nuclear technologies on several criteria, the most important of them being the technology's safety in terms of proliferation. This procedure is now being used to assess current and future nuclear technologies.[57] Clearly, it would

[54] Permanent Mission of the Russian Federation to the International Organizations in Vienna, *Rossiyskaya Federatsiya i situatsiya v oblasti.*

[55] Indeed, IAEA actions with respect to nuclear technology smuggling are, themselves, quite modest.

[56] Russian Foreign Ministry, "International Atomic Energy Agency (IAEA)," Russian Foreign Ministry website, March 11, 2011.

[57] Permanent Mission of the Russian Federation to the International Organizations in Vienna, *Rossiyskaya Federatsiya i situatsiya v oblasti.*

make sense to use the same approach for developing the aforementioned nuclear education and training criteria.

During a visit to Moscow of the IAEA Director General, Yukiya Amano, in May 2013, Russian and IAEA representatives reiterated the importance of continued cooperation in this area. Amano met Sergey Ivanov, the chief of staff of the presidential administration of Russia, to discuss the implementation of several projects as part of the program of technical cooperation with the IAEA. The two also spoke about the use of nuclear technologies in areas other than nuclear energy.[58] During Amano's meetings with Russian officials and representatives of the expert community, emphasis was given to the need for cooperation in preventing nuclear technology leaks, especially during the implementation of the INPRO project.[59]

Currently there are preconditions for intensifying Russia's nonproliferation cooperation with the IAEA. Russia refused to participate in the last Nuclear Security Summit in 2016, and will focus on conducting nuclear security projects together with the IAEA instead.[60]

Practical Russian efforts to prevent the appearance of a black market for nuclear technologies include such initiatives as the establishment of the IUEC and the removal of nuclear fuel from countries that have Soviet or Russian-made reactors. The implementation of the former initiative began in 2007, when the IUEC was set up in Angarsk. At present, the center provides uranium-enrichment services to Ukraine,[61] Kazakhstan, and Armenia. If other countries were to join the IUEC, such a move would strengthen the nonproliferation regime because the new participating nations would have no need to develop sensitive uranium-enrichment technologies.

[58] The Permanent Mission of the Russian Federation to the International Organizations in Vienna, "Sergey Ivanov, IAEA Director-General to Discuss Implementation of the Technical Cooperation Program," May 17, 2013, http://rusmission.org/5/1/2554.

[59] The Permanent Mission of the Russian Federation to the International Organizations in Vienna, "IAEA Chief Visits MGIMO University," May 21, 2013, http://rusmission.org/5/1/2559.

[60] Dmitry Kovchegin, Interview in *Yaderny Kontrol* newsletter (in Russian). *Yaderny Kontrol*, no. 2 (461), February 2015. Available at: www.pircenter.org/articles/1796-nauchno tehnicheskoe-sotrudnichestvo-rassmatrivalos-rossijskoj-storonoj-v-kachestve-prioritet nogo.

[61] Russia continued to fulfill its obligation to deliver nuclear fuel to Ukrainian nuclear power plants even after the beginning of the so-called Ukrainian crisis. See: Mikhail Lysenko, "Karavan Rossiyskoy yadernoi energetiki idyot vperyod," [The Caravan of Russian Nuclear Energy Moves forward], *Security Index*, vol. 20, no. 4 (111), Winter 2014, p. 13.

In the context of international efforts against the black market for nuclear technologies it is important to note the Russian steps to address this problem in the Commonwealth of Independent States (CIS) and the Eurasian Economic Union (Russia, Belarus, Kazakhstan, Armenia, and Kyrgyzstan). Russia is currently implementing a program of long-term cooperation on WMD nonproliferation with the CIS states, approved by the Russian president in 2003. It includes a series of measures to provide CIS countries with consultation services and expertise to improve their national legislation on WMD nonproliferation and export control. The program emphasizes cooperation in preventing any cases of illegal circulation of dual-use products and technologies.

Russia and several CIS states are undertaking important efforts to harmonize their national export legislation, especially as part of the Eurasian Economic Union. To that end, Russia has developed a model piece of export-control legislation. On the one hand, this measure is a constructive step to prevent the appearance of a nuclear technology black market in the former Soviet countries. On the other hand, many experts say that practical implementation of this measure may be difficult. The Russian export-control system is rather cumbersome and prone to excessive bureaucracy – unlike, for example, the system adopted in Kazakhstan, which is more streamlined but no less effective.[62] There seem to be several reasons for the complexity of the Russian system. They include not only the unwieldiness of the Russian bureaucratic machinery, but also the huge Russian territory, which presents additional difficulties in implementing export controls and requires additional measures. It is therefore quite obvious that even if the problem with bureaucracy can be dealt with, the Russian export-control system can never become as streamlined as similar systems in Kazakhstan or even smaller countries. The aim should therefore be not to standardize export-control legislation (by using the Russian, Kazakh, or any other model as a universal template) but to coordinate joint measures to implement the existing laws.

The 2006 White Paper states that traditional anti-proliferation mechanisms are not sufficient to prevent the appearance of black markets.[63] It notes the promising potential of new international mechanisms against proliferation, such as the Proliferation Security Initiative, which was launched by the United States in May 2003. The goal of the initiative is

[62] Sokov, "Russian's White Paper on WMD Nonproliferation."

[63] Permanent Mission of the Russian Federation to the International Organizations in Vienna, *Rossiyskaya Federatsiya i situatsiya v oblasti.*

to step up efforts against the proliferation of WMD and delivery systems by tightening controls over the transportation of WMD materials and related technologies and preventing their trafficking. In Russia, the main efforts in this area are being undertaken as part of the Global Initiative to Combat Nuclear Terrorism (GICNT).

The NATO–Russia Council (NRC) was another practical mechanism for augmenting the nonproliferation regime. Currently, the Ukrainian crisis complicates the dialogue between Russia and NATO. However, the common terrorist threat may create preconditions for the renewal of limited Russia–NATO cooperation to fight against the Islamic State, which is prohibited in Russia. The Islamic State expressed its interest in acquiring weapons of mass destruction. Thus, it is highly important to prevent the leakage of sensitive nuclear technologies to the Islamist terrorists. It appears that in the near future Russia and NATO may cooperate to avoid this threat despite ongoing tensions regarding Ukraine. Before the Ukrainian crisis Russia and NATO accumulated valuable experience in cooperation aimed at stopping black-market nuclear technology networks. Until recently the NATO–Russia Council was a platform for the exchange of opinions on global trends in the proliferation of WMD and delivery systems. The parties were also discussing possible joint political initiatives to promote effective multilateral efforts against proliferation.

To summarize the Russian stance on preventing any nuclear technology leaks in other countries, the following conclusions can be drawn. Even though Russia declares that it is concerned by the possibility of such leaks, overall it is less active in this area of the international arena than the United States. That is not necessarily a negative thing. For example, unlike Russia, the United States is very active on the issue of international sanctions for any violations of export-control regimes. That does not mean, however, that Washington's tough stance is actually helping international efforts against the black market for nuclear technology. Russia's more cautious approach to sanctions, especially sweeping economic sanctions, which is based on Moscow's rejection of the use of force in international affairs, appears to be more balanced and constructive than the position of the United States.

At the same time, it should be recognized that Russia could work more energetically with other nuclear powers in stopping the nuclear black market. While Russia is undertaking efforts against the nuclear black market, it focuses mainly on its own territory and that of the Eurasian Economic Union countries. It is also undertaking some limited measures

as part of the INPRO project, which is being carried out in cooperation with the IAEA – but that is about the whole scope of its international efforts in this area. Obviously, that is not enough. This chapter therefore recommends a greater focus on such an important component as international cooperation in developing a single set of criteria for nuclear education and training.

For now, Russia prefers to keep its involvement in international efforts against the nuclear black market limited to information exchange. Russia had considered more active efforts through the Global Partnership Against the Spread of Weapons and Materials of Mass Destruction (a G8 initiative). The difficult political situation caused by the crises in Ukraine and the Middle East changed those Russian plans. The G8 summit in Sochi in 2014 never took place. Instead, Russia was out of that club, and will not be back.

Disagreements between Russia and the western countries create obstacles for effective international cooperation in the nuclear security field. However, the positive past experience of Russia's nuclear security cooperation with the West, as well as the new common terrorist threats, may create preconditions for unifying the efforts of Russia and the western countries in their struggle against illicit trafficking of sensitive nuclear technologies.

CONCLUSIONS

We estimate the probability of any incidents of illicit trafficking of nuclear technologies in Russia as low. Nevertheless, as this study has demonstrated, there is still a certain risk of potentially weapons-usable nuclear technologies and equipment falling into the wrong hands. These threats are actually part of the reason why there is still a risk of nuclear technology leaks in Russia.

Of course, that risk remains purely hypothetical at the moment. That conclusion is based on the fact that there have been so few documented cases of serious nuclear technology leaks in Russia over the past 25 years. There have only been some incidents involving illegal trade in conventional weapons and missile technology. There were a few cases of nuclear technology leaks as well, and not all of them have become public knowledge. Nevertheless, as far as we can judge, all – or almost all – of those cases have been solved, and no catastrophe has come about. There have been some concerns about the possibility of Russian weapons scientists leaving for countries suspected of proliferation ambitions after the break-

up of the former Soviet Union. However, we suggest it is not clear that this threat has ever actually materialized, thanks in large part to the work of the ISTC.

Russia is undertaking energetic efforts against corruption, a negative phenomenon that can lead to the appearance of smuggling rings dealing in conventional weapons as well as nuclear technologies. The problem of corruption in the nuclear domain was addressed by the Comprehensive Program against Corruption and Smuggling in the Nuclear Complex for 2012–13. Russia is undertaking anti-corruption measures not only at home but also in the international arena, making use of its clout at FATF and the related regional organizations.

Russia is also taking specific practical steps against the nuclear black market with initiatives such as the IUEC.

To summarize, even though there are certain risks and problems, incidents of illegal circulation of sensitive technologies in Russia have been minimized; they are sporadic and do not have an organized pattern. Russia is currently making progress toward fully eliminating the remaining risks of the appearance of nuclear black markets. So far, Russian efforts have been more successful on the domestic front. Nevertheless, Russia is also undertaking effective steps against the nuclear black market beyond its own borders, especially in the former Soviet countries, although there is certainly room for improvement in this regard.