Nuclear security in Russia: can progress be sustained?

Nuclear security in Russia: can progress be sustained?

Matthew Bunn and Dmitry Kovchegin

***Nonproliferation Review,* Vol. 24, Nos. 5-6, pp. 527-551**

(This is the Author's Accepted Manuscript before final editing; the final version is available at https://doi.org/10.1080/10736700.2017.1461734.)

ABSTRACT

Nuclear security in Russia has continued to evolve since the suspension of nearly all U.S.-Russian nuclear security cooperation in 2014. But the United States and the rest of the world now know much less about the directions of this evolution. This article assesses the current state of nuclear security in Russia, based on an examination of key drivers of Russia's nuclear security system, from allocation of resources to regulatory oversight. It then outlines four scenarios for the future of evolution of nuclear security in Russia, describing potential causes, implications, and observable indicators for each scenario. It closes with recommendations designed to maximize the chance of Russia moving on to a path of continuous improvement of nuclear security.

KEYWORDS: Russia; nuclear security; physical protection; material control and accounting; cooperation.

At the 2010 Nuclear Security Summit, the assembled leaders—including Russian President Dmitry Medvedev—agreed that "nuclear terrorism is one of the most challenging threats to international security, and strong nuclear security measures are the most effective means" to prevent it.[1] The effects of a terrorist attack using a nuclear explosive would reverberate throughout the world, giving all countries an interest in ensuring that states with nuclear weapons, weapons-usable nuclear materials, and major nuclear facilities protect them effectively. Unfortunately, however, much of the world knows little about how Russia— the country with the world's largest nuclear stocks, dispersed throughout the world's largest number of facilities—is fulfilling its nuclear security responsibilities

[1] US Department of State, "Communiqué of the Washington Nuclear Security Summit," April 13, 2010, < http://obamawhitehouse.archives.gov/the-press-office/communiqu-washington-nuclear-security-summit>. For a recent summary of the global nuclear-security picture, see Matthew Bunn, Martin B. Malin, Nickolas Roth, and William H. Tobey, *Preventing Nuclear Terrorism: Continuous Improvement or Dangerous Decline?* (Cambridge, Mass.: Project on Managing the Atom, Belfer Center for Science and International Affairs, Harvard Kennedy School, 2016), http://belfercenter.ksg.harvard.edu/files/PreventingNuclearTerrorism-Web.pdf.

Matthew bunn@harvard.edu; kovchegin@yahoo.com

Such information is no longer being made available as part of U.S.-Russian nuclear security cooperation, as since 2014 there has been a cutoff of all but a few elements of that work.[2] Russia's December 2014 decision to suspend nuclear security cooperation – following an earlier U.S. suspension of nuclear energy cooperation as part of its response to Russian actions in Ukraine – had multiple causes, including US–Russian political tensions, Russian concerns over US experts visiting sensitive Russian nuclear sites, and Russia's rejection of the overall framing of the cooperation as US "help" to Russia (putting Russia in the position of a weak state needing US assistance to manage its nuclear stocks).[3] To help fill the resulting information gap, this article uses publicly available documentation and interviews to explore the status of nuclear security in Russia in 2017, and its plausible future evolution. While it is difficult to assess the actual effectiveness of nuclear security on the ground, the information available is sufficient to assess key factors that drive the nuclear-security system.

Nuclear security in Russia improved dramatically in the two decades following the collapse of the Soviet Union, as a result of Russia's cooperation with the United States and others, Russia's own efforts, and Russia's economic recovery. The Russian government has repeatedly asserted that nuclear-security systems in Russia are now highly effective. But these security systems must protect against substantial and ever-changing threats. Russia suffers from significant terrorist activity, with Islamic extremism spreading from the Caucasus to many other areas of Russia, corruption (including in the nuclear sector), and organized criminal activity, all of which could increase both outsider and insider threats to Russia's nuclear stockpiles and facilities.[4]

---

[2] Cooperation on returning Russian-supplied HEU from third countries continues, as do discussions of regulatory issues. For a recent discussion, see Matthew Bunn, "Steps for Rebuilding US–Russian Nuclear Security Cooperation," presented to the 58th Annual Meeting of the Institute for Nuclear Materials Management, Indian Wells, Calif., July 17-20, 2017. For a broader set of proposals for US–Russian cooperation in a range of nuclear areas (to which both of the authors contributed), see *Pathways to Cooperation: A Menu of Potential US–Russian Projects in the Nuclear Sphere* (Washington, D.C.: Nuclear Threat Initiative and Center for Energy and Security Studies, February 2017), <http://www.nti.org/media/documents/Pathways_to_Cooperation_FINAL.pdf>.

[3] For accounts of this suspension, see Matthew Bunn, "Rebuilding US–Russian Nuclear Security Cooperation," *Nuclear Security Matters*, January 22, 2015, http://nuclearsecuritymatters.belfercenter.org/publication/rebuilding-us-russian-nuclear-security-cooperation; Matthew Bunn, "Russia Puts a Positive Spin on Nuclear Security Cooperation – Which is Good," *Nuclear Security Matters*, January 23, 2015, <http://nuclearsecuritymatters.belfercenter.org/publication/russia-puts-positive-spin-nuclear-security-cooperation-%E2%80%93-which-good.

[4] See, for example, Alexey Malashenko and Alexey Starostin, *The Rise of Non-Traditional Islam in the Urals* (Moscow: Carnegie Moscow Center, September 2015), <http://carnegieendowment.org/files/CP_MalashenkoUral_Sept2015_web_Eng.pdf>. On corruption, see, for

Nuclear security can never be considered "done." In the face of evolving threats, changing technologies, and newly discovered vulnerabilities, nuclear-security managers must focus on continual improvement. Yet security must constantly compete for resources and attention with other organizational priorities. Complacency about the threat and about the effectiveness of existing security systems can erode nuclear security over time, particularly when organizations are under pressure to do more with less. In 2000, Jens Rasmussen and Inge Svedung argued that accidents are "the effects of a systematic migration of organizational behavior… under the influence of pressure toward cost-effectiveness in an aggressive, competitive environment."[5] The same could be said for security vulnerabilities.

These phenomena exist in Russia, and in every other country. To what extent could erosion be taking place at Russian nuclear sites? The answer is not fully known. There are several clear reasons for concern, in addition to the evolving threats mentioned earlier:

- The end of most US-Russian nuclear-security cooperation deprives Russia of one set of independent voices making nuclear-security suggestions, as well as of the limited funding that was still being provided to some sites.
- As a result of low oil prices and economic sanctions, the Russian government is running a deficit and funding for the nuclear industry has been cut, raising questions about whether funding for nuclear security has been or will also be reduced.[6]
- When most US–Russian cooperation ended, there were additional steps that US experts believed needed to be taken, in a range of areas, at many nuclear sites.[7]

Key drivers within Russia that could push in the opposite direction, toward sustainability and continuous improvement of nuclear security, include:

---

example, Oleg Yegorov, "Head of Russian Anti-Corruption Unit Caught with $140 Million in Cash," *Russia Beyond the Headlines,* September 13, 2016. Russian Prime Minister Dmitry Medvedev has identified corruption as posing a major threat to Russia's national security. See Janet McBride and Michael Stott, "Poverty and Corruption Threat Russia: Medvedev," Reuters, June 25, 2008.

[5] Jens Ransmussen and Inge Svedung, *Proactive Risk Management in a Dynamic Society* (Karlstad, Sweden: Swedish Rescue Services Agency, 2000), quoted in Sidney Dekker, *Drift into Failure: From Hunting Broken Components to Understanding Complex Systems* (Farnham, UK Ashgate, 2011), p. 1.

[6] See Government of the Russian Federation, Ministry of Finance, "Main Directions of Budget Policy for 2016 and Planned Period of 2017-2018," (in Russian), http://www.budget.gov.ru/epbs/content/conn/content/path/Contribution%20folders/documents/Основные%20направления%20бюджетной%20политики%20РФ%20на%202016%20год.pdf.

[7] Interviews with U.S. laboratory experts, September 2016.

- Leadership commitment, threat perception, and security culture;
- Funding and resources, including personnel training;
- Regulatory oversight;
- Threat and vulnerability analyses and testing;
- Consolidation; and
- International cooperation.

This article offers an overview of current Russian nuclear-security approaches and institutions, including an assessment of each of these key drivers of nuclear security. The article then discusses scenarios for the evolution of nuclear security in Russia in the future, describing the drivers that might lead to each scenario, the scenario's implications, as well as indicators outside analysts might use to identify that it was unfolding. Finally, the article offers policy recommendations to maximize the chance that Russian nuclear security will follow the highest-performance trajectories.

In this article, we focus, as the first Nuclear Security Summit did, mainly on security and accounting measures for nuclear weapons and the materials that could be used to make them: highly enriched uranium (HEU) and plutonium separated from spent fuel. These measures are sometimes called nuclear-material protection, control, and accounting (MPC&A). The measures we discuss also address protecting nuclear facilities from sabotage. We do not address in detail measures to provide security for radiological sources, to block illicit trafficking, or to respond to nuclear emergencies, all of which are important but beyond our scope.

Overview of nuclear security in Russia

Unclassified estimates suggest that Russia has some 7,000 nuclear weapons, and stocks of 650-700 metric tons of HEU and 170-190 tons of separated plutonium, enough for many thousands of additional nuclear weapons.[8] Russia has over 40 nuclear-weapon storage sites (in addition to strategic deployment areas), and some of these are large sites with several separate fenced areas.

[8] See Hans M. Kristensen and Robert S. Norris, "Status of World Nuclear Forces" (Washington, DC: Federation of American Scientists, 2017), https://fas.org/issues/nuclear-weapons/status-world-nuclear-forces/; and "Fissile Material Stocks" (Princeton, N.J.: International Panel on Fissile Materials, 2017), http://fissilematerials.org/.

Weapons-usable nuclear materials in Russia are stored and handled in over 200 buildings, ranging from massive plutonium processing facilities in closed nuclear cities to small research facilities using modest amounts of HEU. All told, US–Russian cooperative efforts included security and accounting improvements for some 210 buildings and 97 nuclear-weapon storage areas, representing a large fraction (though not 100 percent) of the total in each category.[9]

Today, Russian nuclear facilities are generally equipped with modern fences, intrusion detectors, barriers, access control systems, vaults, and nuclear-material accounting and control systems. Operators are required to provide protection against a range of both outsider and insider threats. Armed guard forces are in place at nuclear sites. A broad set of nuclear security and accounting regulations, agency rules, site-level procedures, and other guidance is in place.

Nuclear operators in Russia are required to perform in-depth vulnerability assessments (including vulnerabilities to both insider and outsider threats) and address any weaknesses identified. They are also required to test whether their security and accounting systems are functioning. Nuclear staff are paid reasonable wages, on time. Moreover, Russia has significantly reduced the number of locations with nuclear weapons, plutonium, and HEU (although it still has more of these than any other country). For example, over the last twenty years, Russia closed its last plutonium-production reactors and the two major plutonium-reprocessing plants associated with them and reduced the number of nuclear-weapon assembly and disassembly facilities from four to two.[10] In short, Russian weapons-usable nuclear material is much better protected than it was twenty-five years ago. Indeed, some Russian nuclear-security practices are arguably superior to those in the United States, such as conducting no-notice security tests (discussed in more detail below), or placing government agents among the staff at key nuclear facilities to create a difficult-to-quantify additional element of detection and deterrence.

Nevertheless, a number of concerns remain:[11]

---

[9] See Matthew Bunn, *Securing the Bomb 2010: Securing All Nuclear Materials in Four Years* (Cambridge, Mass.: Project on Managing the Atom, Harvard University, and Nuclear Threat Initiative, April 2010), p. 33, and references therein.

[10] Pavel Podvig, "Consolidating Fissile Materials in Russia's Nuclear Complex," *International Panel on Fissile Materials Report*, May 2009, http://fissilematerials.org/library/rr07.pdf (accessed February 18, 2016).

[11] These points are based on 2016-2017 interviews with U.S. national laboratory personnel and discussions with other experts over the last several years.

- *Sustainability.* Will Russia's nuclear organizations sustain and improve security over time? Or will complacency, budget pressures, and other factors lead to erosion? Will Russia's funding for nuclear security be enough? (Security funding may be a particular concern for small sites with modest revenue, such as research reactors.)
- *Insider threats.* Are protections against insider threats sufficient? When US–Russian cooperation was largely suspended, work on several additional steps to cope with insider threats was cut off. At some sites, US experts identified pathways insiders could use to get nuclear material out, such as security gratings over windows that could still be opened from the inside without setting off any alarm. The national material control and accounting regulation, known by its Russian acronym OPUK, requires the use of "two-person rule," but once the two people have entered an area, it does not require that they remain within sight of each other. Russia continues to conduct bulk processing of weapons-usable nuclear material—the activity that creates the most risk of covert insider theft—on a scale of tons of material every year, but there is more to do to ensure that material control and accounting would be sufficient to detect protracted theft occurring in small amounts at a time (another area where important joint work was cut off when cooperation was suspended). In Russia, as in the United States and elsewhere, building a culture in which staff report red flags and concerning behavior in time for the organization to act remains a major challenge.
- *Robust performance testing and assurance.* Russia has been strengthening its approaches to performance testing in recent years, but some US experts still see considerable room for improvement. "Force-on-force" exercises in Russia are mainly carried out to train guard forces, not to actually test the performance of the security system against an intelligent adversary. Tests generally focus on whether equipment is working, not whether intelligent adversaries looking for a way to beat the security system might succeed.
- *Security culture.* US–Russian discussions on approaches to strengthening security culture generated a wide range of ideas, many of which have been implemented at some Russian sites. But changes in organizational culture have to come from site leadership, and it remains uncertain whether all the management of all Russia's

nuclear facilities are really putting in the focused effort needed to build strong security cultures. As one US government expert put it, at many sites it was hard to see "real, tangible evidence of significant change."[12] Belief in the threat is the foundation for a strong security culture, and skepticism about how realistic it is to think that adversaries might attempt to steal nuclear material in today's Russia (as opposed to the Russia of the 1990s) remains widespread.[13] (As discussed below, many officials are more concerned about nuclear sabotage or terrorist use of a radiological "dirty bomb.")

Given these strengths and potential weaknesses of nuclear security in Russia today, we now describe six key drivers of the evolution of Russian nuclear security.

Leadership commitment, threat perception, and security culture

Sustainable nuclear security requires awareness and acknowledgement of the threat and commitment to act on it at all levels—from the country's leadership, to the leaders of nuclear organizations, and to rank-and-file nuclear security personnel.

In Russia, there are a wide range of views on the plausibility of the threat of terrorists acquiring and using nuclear explosives. President Vladimir Putin, in a 2005 joint statement with US President George W. Bush, agreed that this was "one of the gravest threats our two countries face."[14] Anatoly Safonov, while serving as Putin's special representative for counterterrorism (subsequent to his service as acting head of the Federal Security Service, or FSB), warned that "we know for sure, with evidence and facts in hand, about this steady interest and a goal pursued by terrorists to obtain what is called nuclear weapons and nuclear components in any form."[15] Russia is the country that proposed the International Convention for the Suppression of Acts of Nuclear Terrorism (ICSANT), and in 2006, Putin and Bush co-founded the Global Initiative to

---

[12] Interview, April 2015.
[13] Sergei Ivanov, then the Russian minister of defense, summed up a widely expressed (though demonstrably false) Russian view in 2004, asserting that it was "impossible for there to be any loss" of plutonium or uranium, and that there had never been "a single case of so much as a gram being lost." Russian acceptance of cooperative threat reduction assistance, he said, "does not mean that nuclear materials are stored poorly." See Svetlana Babaeva, "Responsible, Rational, With No Fear on His Face," *Izvestia,* trans. by *What the Papers Say*, April 9, 2004.
[14] "Russian-U.S. Joint Statement on Nuclear Security Cooperation" (Moscow: The Kremlin, January 24, 2005), http://en.kremlin.ru/supplement/3562.
[15] "Russian Foreign Ministry Aware of Terrorist Attempts to Obtain Nuclear Weapons—Diplomat," *Interfax,* September 27, 2007.

Combat Nuclear Terrorism (GICNT), which Russia and the United States still co-chair. Many Russian public statements emphasize the importance of nuclear security, with Rosatom—Russia's state nuclear corporation—describing security at its facilities as its "top strategic priority," a "prerequisite for successful performance in the nuclear industry," and noting its commitment to continuous improvement.[16]

Many other officials and managers are more skeptical, however, arguing that it would be extraordinarily difficult for terrorists to get a nuclear bomb or the materials needed to make them, or that it would be "absolutely impossible" for terrorists to make a bomb even if they got the needed material, as Anatoli Kotelnikov, then in charge of security for Russia's nuclear complex, put it in 2002.[17] Overall, most Russian officials see the threats of sabotage of nuclear facilities or terrorist use of a radiological "dirty bomb"—both tactics that Chechen terrorists threatened in Russia—as higher priorities than the threat of nuclear material theft. And while Russia's leaders often highlight the terrorist threat, they also emphasize the strength of Russia's counterterrorism and nuclear-security policies, sometimes projecting a sense of complacency rather than vigilance to target audiences.

In international discussions, Russia generally prioritizes nuclear-energy promotion more than nuclear security. This includes aggressive exports to countries with questionable nuclear security—although these export contracts typically include support for developing nuclear-security infrastructure in the recipient country.

The Russian government sees its nuclear complex, and its defense component in particular, as a critical national asset, deserving effective protection from both safety and security incidents. For years, the Russian nuclear industry has enjoyed substantial government financial support. Since the early 2000s, the Russian government has passed several laws to strengthen safety and security and to clarify oversight and inspection authorities. While early regulatory legislation treated the nuclear industry as no different from others, later legislation called out the nuclear industry separately, to reflect the special care warranted by its special status and

---

[16] Rosatom, "Protection of Nuclear Materials and Facilities" (Moscow: Rosatom, no date), http://www.rosatom.ru/en/about-us/protection-of-nuclear-materials-and-facilities/. One would be hard-pressed to find a comparatively fulsome commitment to security in the public material of most Western nuclear companies.
[17] Aleksandr Khinshteyn, "Secret Materials," trans. BBC Monitoring Service, "Russian Central TV," November 29, 2002.

hazards.[18] The Russian government has allocated funding for nuclear safety and security through both regular budget expenditures and federal targeted programs. In 2014, President Putin highlighted the importance of the nuclear-weapons complex with a decree establishing the special status of "federal nuclear organization" for Russia's core weapons complex facilities; these facilities are expected to receive additional funding and special security measures.[19]

Individual nuclear sites represent the next level where security culture and leadership are critical to effective security performance. The variation in approaches to nuclear security at individual nuclear sites provides clear evidence of the importance of site leadership's commitment to nuclear security. For example, after a well-publicized theft of weapon-grade HEU at the Luch Production Association in the city of Podolsk, near Moscow in 1992, Luch went from being a place with weak security to being a model site, largely because of an effective group of site leaders who made site security a priority and committed personnel who worked with them.[20]

Unfortunately, there are only limited incentives for nuclear managers to focus on nuclear security. In particular, Rosatom gives greater priority to profitability than to security in a set of key performance indicators it has established for officials leading nuclear facilities.[21]

Attitudes toward nuclear security also vary from highly committed to complacent among individual staff at nuclear facilities. Some continue to side with Kotelnikov in believing that terrorists could not possibly make a nuclear bomb even if they got nuclear material. Even more dismiss the idea that thieves could ever overcome the security systems at Russian nuclear sites to steal nuclear material.

For years, Russian and US officials worked together to establish security culture programs, with a variety of training and other measures intended to motivate personnel to give

---

[18] For example, compare the original and currently valid amended versions of Federal Law No. 184, December 27, 2002, "On Technical Regulations" (establishing the procedural requirements for establishing mandatory technical rules) and the Federal Law No. 294, December 26, 2008 "On Protecting Rights of Legal Entities and Individual Entrepreneurs during Implementation of State Oversight and Municipal Control," establishing requirements for implementing oversight activities.

[19] Office of the Russian President, "On Federal Nuclear Organizations," Decree No. 467, June 26, 2014.

[20] The story of nuclear security upgrades at Luch is well covered in over 20 papers delivered by the site team in charge of nuclear security to INMM Annual Meetings in 1996-2011. Available at http://www.inmm.org/source/proceedingssearch/

[21] Observations from comments of Russian nuclear-industry experts at multiple events.

high priority to security. Rosatom ultimately decided to establish security-culture coordinators at each of its major sites with weapons-usable nuclear material. Nevertheless, the limited efforts undertaken so far are not likely to be sufficient to result in substantial improvements across Russia's far-flung nuclear complex. Some of these programs were imposed on nuclear sites, often without sufficient regard for long-standing Russian approaches to managing the "human factor" in nuclear safety and security, and were not accepted by many nuclear employees. In some cases, these initiatives received only modest support from site management, and incentives for staff to invest effort on security vigilance are limited. The nuclear-security culture regulation developed by Rosatom for its sites focuses more on specific procedures sites should implement than the strength of the security culture to be achieved, and is is not based on the best practices captured in the International Atomic Energy Agency (IAEA)'s nuclear-security culture guidelines.[22]

[22] V. Prostakov, Rosatom; A Bushlya, Rosatom; N. Geraskin, MEPhl; T. Piskureva, FSUE "RISI"; V. Kornelyuk, MATI "Atomenergo". Organizational Order and Testing Methodology of the Culture Level at Nuclear Site. In *Proceedings of the 52nd Annual Meeting of the Institute of Nuclear Materials Management, 17-21 July 2011, Palm Desert, California* (Northbrook, Ill.: INMM, 2011). For the IAEA recommendations on strengthening nuclear security culture, see International Atomic Energy Agency, "Nuclear Security Culture: Implementing Guide," (Vienna: IAEA, 2008), <www-pub.iaea.org/MTCD/publications/PDF/Pub1347_web.pdf>.

Nuclear security resources

Resources—including both funding and trained personnel—are another key driver of nuclear security and a key indicator of priorities. In cutting off most US–Russian nuclear-security cooperation, Russia indicated it would pay for remaining work itself.[23] Rosatom has reported that it is investing in a variety of security improvements, including physical protection upgrades for forty-nine buildings and 28 kilometers of site perimeter fencing in 2016 alone.[24] But it is not yet clear that Russia has completed all the work that US and Russian experts agreed needed to be done, or that the Russian government and its facilities will allocate sufficient funding to sustain effective nuclear security and accounting measures over time.

Russian legislation requires nuclear-facility operators to have sufficient financial capabilities to ensure safe and secure operation.[25] This requirement, however, is not subject to any substantial validation during operator licensing and inspections.[26]

There is no question that the Russian government has the resources to provide for effective nuclear security if it chooses to allocate them. The costs of nuclear security are small if judged at a national level, probably not amounting to more than a few percent of the Russian nuclear complex's annual operating expenses (possibly less). But security costs may loom large for individual facilities—especially small research facilities with modest revenues—and in some cases, facilities may face much of the burden of finding the funds for nuclear security themselves.

In Russia, there is no single nuclear-security budget: nuclear-security funding is spread among accounts at individual sites, at Rosatom, at the Ministry of Defense (MoD), at other agencies managing nuclear material and facilities, at Rostechnadzor (the agency that includes Russia's civilian nuclear regulators), at the Ministry of Interior (whose troops contribute to guarding nuclear materials), at security agencies involved in nuclear security (such as the FSB), and more. Nuclear facilities are expected to use their revenue to adopt measures that ensure that

---

[23] For a discussion with links to the Russian statement, see Bunn, "Russia Puts a Positive Spin on Nuclear Security Cooperation – Which is Good."
[24] *Rosatom Annual Report: 2016* (Moscow: Rosatom, 2017).
[25] See Article 34 of the Federal Law "On Atomic Energy Use."
[26] See "Administrative Procedures for the Performance of the State Service of Licensing of Activity in the Area of Atomic Energy Use by the Federal Service for Environmental, Technological and Nuclear Oversight (Moscow: Rostechnadzor, October 8, 2014).

they comply with relevant regulations and agency requirements. In addition, sites receive funding from the federal government for some nuclear-security efforts, and there is a reserve fund for nuclear security that sites both contribute to and receive funding from.[27]

Russian legislation requires nuclear sites to contribute specified amounts, amounting to up to 2 percent of their income, to a special reserve fund for MPC&A, managed by the agency to which they report (Rosatom, for most nuclear facilities).[28] Each agency managing nuclear sites determines the specific amounts within the 2-percent ceiling that each of their sites has to pay. The agency then distributes the special reserve funds in accordance with site requests and its own needs analysis, so sites may get either more or less than they contributed in a particular year. This process facilitates funding for capital-intensive improvements that might require a site to spend more than usual for a few years.

There are also mechanisms for Rosatom and other agencies managing nuclear sites to request nuclear-security funds from the federal budget, as part of broader budget planning. Federal budget funding can be provided through the regular budget or through "federal targeted programs"—multi-year funding mechanisms aimed at resolving specific issues.

Because of the large number of different accounts that contribute to nuclear security, and the lack of transparency in them, it is difficult to estimate overall spending on nuclear security in Russia. But the requirement to publish data on essentially all non-sensitive procurements by Rosatom nuclear sites, including MPC&A procurements, provides a window on at least a portion of nuclear-security spending.[29]

In 2015, Rosatom organizations published information on over 52,000 awarded contracts.[30] Several hundred of these were directly related to MPC&A, ranging from a $7.9 million contract for guarding services for the Mining and Chemical Combine in Zheleznogorsk

---

[27] Government of the Russian Federation, "Rules for Financial Contributions of Organizations Operating High-Radiation and Nuclear-Hazardous Facilities and Sites (except Nuclear Power Plants) to Reserves Intended for Ensuring Safety/Security of These Facilities and Sites at All Stages of Their Lifecycle and Development," Government Decree No. 576, September 21, 2005.

[28] Government of the Russian Federation, "Rules for Financial Contributions of Organizations Operating High-Radiation and Nuclear-Hazardous Facilities and Sites (except Nuclear Power Plants) to Reserves Intended for Ensuring Safety/Security of These Facilities and Sites at All Stages of Their Lifecycle and Development," Government Decree No. 576, September 21, 2005.

[29] This data is available on-line, at Rosatom, "Закупки," (Procurements), http://zakupki.rosatom.ru/Web.aspx?node=archiveorders.

to a $380,000 contract for physical protection maintenance at Atomflot (which manages Russia's nuclear-powered icebreakers).[31] Overall, total funding for nuclear-security procurements at Rosatom sites appears to be in the range of hundreds of millions of dollars annually.

While the Russian nuclear industry seems to enjoy substantial funding support from the government, as well as through profitable commercial activities, its future might not be as bright. Russian authorities have already acknowledged that financial problems and a decline in budget expenditures in the coming years are highly likely.[32] Other major sources of funding—the facilities' own funds and their contributions to the special MPC&A reserve fund—will depend on the profitability of Russian nuclear-industry activities. With the global slowdown in nuclear power after the Fukushima accident, Rosatom itself providing much of the financing for its reactor exports, vanishing demand for reprocessing, and historically low prices for uranium and enrichment services, that profitability may be called into question.

Effectively trained personnel are also a key resource required for sustainable nuclear security. Unlike many countries, Russia now has training requirements for people in particular MPC&A jobs, with both centralized and site-based training available, as well as degree programs at universities such as the Moscow Engineering Physics Institute (also known as the National Research Nuclear University). These training programs, however, were established with substantial US assistance, and some appear to be struggling to provide the same level of instruction in the absence of US funding.

Regulatory oversight

In a resource-constrained environment, many nuclear managers will only invest in expensive nuclear-security measures if the government requires them to do so. Hence, strong and effectively implemented regulations, including independent oversight, are critical to achieving effective and sustainable nuclear security. Nuclear-security regulation includes documents establishing requirements for specific activities; licensing; inspections, to validate the operator's

[31] Converted at currency exchange rates at the contract signature date for the Zheleznogorsk contract and the procurement notification date for the Atomflot contract.
[32] "Main Directions of Budget Policy for 2016 and Planned Period of 2017-2018."

compliance with established requirements; and approaches to convincing operators to comply (including punishments for violations).

In Russia, Rostechnadzor regulates civilian nuclear-power reactors and other civilian uses of nuclear technologies, while the Department of State Oversight over Nuclear and Radiation Safety and Security of the Russian MoD (known by its Russian acronym UGN) regulates defense applications (including both MoD's nuclear weapons and materials and Rosatom activities involving nuclear weapons and naval fuel), with substantial support from Rosatom. There is some uncertainty about the exact point at which nuclear material crosses the "border" between these two regulatory domains, and some facilities operate under both civilian and defense licenses.

The regulatory basis for nuclear-materials security in the civilian domain is well established in Russia. It is based on an overarching law ("On Atomic Energy Use," first issued in 1995); government-wide decrees outlining general approaches (particularly one on physical protection and one on material control and accounting);[33] federal norms and rules (known by their Russian acronym, FNP), setting out somewhat more detailed requirements, similar to the US Nuclear Regulatory Commission's regulations issued under Title 10 of the Code of Federal Regulations; agency-level rules, providing more specific requirements; and technical guidance on methods to comply with the rules and regulations.

The two key FNPs establishing MPC&A requirements are NP-083-15, "Requirements for the Physical Protection Systems of Nuclear Sites, Nuclear Materials, and Nuclear Material Storage Sites," and NP-030-12 "Basic Rules of Nuclear Materials Accounting and Control" (known by its Russian acronym OPUK). The latest versions of these documents were introduced in 2015 and 2012, respectively. There are several other FNPs applicable to MPC&A, establishing requirements for individual elements of MPC&A systems.[34]

---

[33] "Rules of Physical Protection of Nuclear Material, Nuclear Facilities, and Nuclear Material Storage Points," approved by Government Decree No. 456, July 19, 2007; and "Regulation of the System of State Accounting and Control of Nuclear Materials," approved by the Government Decree No. 352, May 6, 2008. These two decrees list the stakeholders for nuclear activities, enumerate their roles and responsibilities and requirements for their interactions, and establish key requirements for the organization of physical protection and MC&A at nuclear sites.

[34] These include, for example, NP-085-10, "Requirements for the Physical Protection of Nuclear Powered Vessels and Nuclear Material Transport Vessels"; NP-072-14, "Rules for Reclassifying Nuclear Material as Radioactive Substances or Radioactive Waste"; and NP-081-07, "Requirements for Organization of Material Balance Areas." There are other FNPs that primarily cover non-MPC&A topics, but contain some provisions related to MPC&A.

To facilitate compliance, Rostechnadzor issues guidelines on various MPC&A topics. These guidelines are not mandatory but provide approved methods for complying with the FNPs.[35] Facilities that build and operate their MPC&A systems according to the guidelines find it easier to pass through their licensing process and Rostechnadzor inspections, while facilities must get formal Rostechndazor approval for taking an approach other than one suggested in the guidelines.

Before issuing a license to operate with nuclear materials, Rostechnadzor reviews a detailed justification from the applicant showing how it will ensure safe and secure operation. Rostechnadzor will also conduct inspections to verify the applicant's information and validate that the safety and security measures are sufficient. Licensing regulations require applicants to provide detailed information about their MPC&A measures, but it is not clear how detailed the information in these justifications actually is, or how much rigor Rostechnadzor applies to examining it.

Once issued, a facility's license is accompanied by a set of license-validity terms, elaborating on the higher-level FNPs, that the facility must comply with during operation. These license-validity terms, including MPC&A requirements, are unique for each site. Rostechnadzor then inspects to confirm that the licensee is complying with regulatory requirements and its license-validity terms. MPC&A issues can be checked during regular comprehensive inspections, as well as during targeted MPC&A inspections. Rostekhnadzor can also conduct an emergency inspection if there is evidence raising a concern.

Rostechnadzor has the right to impose sanctions for violations, including fines, penalties for site management, or even shutting facilities. The first instance of noncompliance rarely results in sanctions, however. Instead, Rostechnadzor directs the site to correct the violation or implement compensatory measures and to prepare a plan and schedule for doing so. Then Rostechnadzor can conduct additional inspections to verify that the plan has been implemented, and would then impose sanctions if the facility failed to do so.

Despite Rostechnadzor's right to shut facilities down over MPC&A violations, there have been few cases of that so far, and other sanctions may not always be enough to convince

[35] There are several dozen of these guidelines, and many of them are publicly available at http://gosnadzor.ru/nuclear/materials/acts/.

facilities to comply. Much more severe sanctions, including imprisonment, could be applied under the Criminal Code, for example in cases in which operators willfully created dangerous vulnerabilities in violation of the law, but Rostekhnadzor has no authority to impose criminal penalties, instead having to refer such cases to the General Prosecutor's office.

For defense nuclear activities, there is still no umbrella federal law, similar to the law "On Atomic Energy Use," that would establish fundamental safety and security requirements. At the level of regulations, only the government-established Rules of Physical Protection apply to both civilian and defense domains.

Defense nuclear activities, appear to be well-covered by agency-level rules. Rosatom agency-level regulations apply to all facilities reporting to Rosatom, whether defense or civilian. A significant volume of Rosatom agency-level regulations governing MPC&A activity have been developed within the framework of US–Russian nuclear-security cooperation, including Rosatom's Order 550—probably the most extensive and detailed physical-protection regulation in Russia.[36] Rosatom is in charge of licensing non-MoD organizations involved in defense nuclear-energy use, and it has the authority to impose its agency requirements on non-Rosatom organizations in the defense sector through license validity terms. MoD organizations are governed by internal MoD regulations, but the specifics of these are not available in the public domain.

While Rosatom handles licensing for defense nuclear activities, MoD's UGN unit is in charge of inspections, though for non-MoD organizations, it is likely that Rosatom plays a major role in oversight as well, as government regulations give the licensing authority (Rosatom) the right to conduct inspections, order corrective actions, and impose sanctions for violations of licensing requirements and license validity terms.

In addition to regulatory oversight, most of the agencies with nuclear facilities reporting to them have some sort of agency-level MPC&A monitoring at their own facilities. Rosatom, in particular, has a well-established agency-level MPC&A inspection system organized by Rosatom departments in charge of physical protection and materials control and accounting. This system is, to a large extent, independent, as the departments in charge of specific monitored sites are not

[36] "General Requirements for Physical Protection Systems at Nuclear Hazardous Facilities" (Moscow: Rosatom, 2001). Rosatom developed a revised version of this old rule with U.S. support, but it has not yet been enacted.

involved. An inspection team typically consists of Rosatom headquarters personnel, as well as subject matter experts from other Rosatom sites, thus turning this effort into something akin to a peer-to-peer review. These Rosatom reviews often take a week or more, going into greater depth than typical Rostechnadzor inspections do, and are designed more to help the site improve than to find violations. Such inspections result in formal reports capturing the status of MPC&A at the inspected site and providing recommendations for improvement. While formal sanctions are not available as part of this process, Rosatom hires and fires nuclear site management and controls most of the sites' budgets, giving it substantial influence.

There are more important specifics of MPC&A regulations than there is space to describe here, but a few broad requirements are worth noting. High-consequence sites are required to put in place security systems able to cope with specified levels of adversary capability (reviewed by regulatory authorities) and to adjust these security systems over time as threats evolve. To ensure effectiveness, the rules require regular checks at various levels (including regulatory inspections, agency monitoring, and regular checks by site management). Sites must eliminate any deficiencies identified during these inspections through corrective and compensatory measures. In addition, as described below, regulations require that protection systems be developed and upgraded based on analyses of potential vulnerabilities to adversary threats and the effectiveness of security systems in addressing them; once security systems are in place and operating, such assessment must continue at least at a set frequency.

These regulatory approaches have significantly strengthened nuclear security in Russia, but several remaining issues are worth noting. First, as in many countries, the regulations are primarily compliance-based rather than performance-based—focusing on whether a barrier or an alarm complies with specified rules more than whether the overall system is effective. Second, there are issues about how fully and effectively all the rules are implemented day to day, as they are quite complex, existing in multiple layers of documents, and Russian regulators have less power and fewer resources, and sometimes less expertise, than institutions like Rosatom or the MoD that they are trying to regulate. Third, the requirements for vulnerability analyses and effectiveness evaluations cover sites' physical protection systems but do not cover nuclear materials control and accounting systems. Fourth, as noted earlier, both the two-person rule requirement and requirements for accounting systems able to detect and localize protracted thefts

of nuclear material could be improved. As the latest version of OPUK, in particular, is already five years old, it is time to begin considering revisions that might address such issues.

Some reports have suggested that in some cases, inspectors who realized a facility did not have the resources to comply with a particular requirement have avoided writing up the violation, giving the facility more time to comply, or even ignoring the violation entirely.[37] Moreover, where inspectors are paid tens of thousands of dollars a year and may find violations that would cost millions of dollars to fix, there is an obvious potential for corruption. Indeed, one Ministry of Interior officer was arrested for soliciting tens of thousands of dollars to overlook security violations in the closed city of Snezhinsk.[38] Such reports have been rare to date, however, and Russian regulators have an active anti-corruption program.[39]

Security assessment and performance testing

Rigorous assessment and testing is another key driver of nuclear-security performance. As noted earlier, Russian nuclear facilities are required to have systems in place to defend against specified adversary capabilities and tactics, and to undergo assessments to confirm that the systems are effective against the threat. If an evaluation finds that the security system's effectiveness is not sufficient, Russian regulations require that upgrades be implemented. Similarly, if a threat assessment shows that the threat has changed, then the regulations require the site to undergo a new evaluation of its security system's effectiveness.

In the Russian system, the kind of evaluation usually described in the United States as "vulnerability assessment" is broken into two parts. The first, "vulnerability analysis," includes characterizing the site; identifying the assets to be protected (e.g., nuclear materials, critical facility elements, classified data) and their location on the site; developing "intruder profiles" (descriptions of potential adversaries to be protected against, with their capabilities and tactics); and determining the consequences of potential unauthorized actions. The second, "effectiveness evaluation," involves estimating the probability that the security system will succeed in defeating adversaries with capabilities and tactics specified in the intruder profiles.

---

[37] Interview with NNSA official, May 2011.
[38] "An Employee of the Department of Classified Facilities of the MVD Was Arrested in Snezhinsk: What Incriminates the 'Silovic'," *Ura.ru*, May 29, 2008.
[39] For relevant documents, see the Rostekhnadzor website, http://gosnadzor.ru/nuclear/.

Vulnerability analysts develop intruder profiles based on the list of threats to nuclear sites established at the federal level (the national-level design basis threat), adapted for the specifics of each site. Local law enforcement and intelligence authorities are involved in developing the intruder profiles for specific sites. The results of this vulnerability analysis serve as a basis for designing security systems to defeat the types of adversaries included in the intruder profiles.

As in the US approach to vulnerability assessment, effectiveness evaluators base their assessment on analysis of the most vulnerable pathways to the protected asset, using measured or estimated values for the probability of detection, the intruder delay time for various elements of the physical-protection system, and the response force action time specific to the evaluated system.

In accordance with Russian regulations, such evaluations must be carried out in first designing a physical-protection system, at a minimum frequency thereafter, and whenever there are changes in the physical-protection system, the threat and intruder profiles for the site, or the category of assets subject to protection (nuclear materials, critical facility elements, classified data) and their location on the site.

Many of the elements of an effective system for evaluating and testing nuclear-security system performance are in place in Russia. But some key issues remain:

- Until new regulations were issued in 2015, there was no regulatory requirement that an effectiveness evaluation needed to use actual data from testing of the real system, rather than "paper" data obtained from manufacturer equipment documentation, system design documentation, qualification requirements with which response forces personnel must comply, or guesses by experts.[40] In particular, the new regulations require that "source data used for evaluation of physical protection system effectiveness indicators must correspond to actual parameters of the physical protection system equipment, adversary and response force tactics, and must be validated through drills and exercises." Sites are typically allowed some lead time to meet new requirements, however, and it is not clear whether this requirement is yet being fully enforced.

[40] Such a requirement was introduced only in late 2015, in the latest revision of the physical protection federal rules. See NP-083-15, "Requirements for Physical Protection Systems of Nuclear Sites, Nuclear Materials, and Nuclear Material Storage Sites", approved by Rostechnadzor Order No. 343, September 8, 2015.

- The "attempt-to-defeat," or "red teaming" approach to testing equipment and personnel— which can help reveal what would happen if intelligent adversaries were looking for ways to defeat the security system— is not common in Russia. Instead, tests are typically designed to confirm that equipment performance meets key criteria taken from documentation; that is, the testing demonstrates compliance with rules more than effectiveness in defeating realistic adversaries.
- Russian organizations conduct force-on-force drills, but their major goal is training, not performance testing; often, the outcome of the drill is determined in advance.

Until 2014, the US Department of Energy was working with Russian organizations to implement a range of performance testing best practices at Russian sites. Over years of discussions and best-practice exchanges, Russian organizations' understanding of and commitment to performance testing has been growing, but genuinely realistic performance testing is still far from being common practice.

There is evidence, however, that Russia does sometimes implement a form of performance testing that is different from (and arguably more realistic than) its US counterpart.[41] A story published on the FSB website back in 2001 describes a practice carried out by FSB special forces, known as scenario-based tests, in which special forces played intruders. The story notes that in a test, the "intruders" successfully seized a nuclear-power plant and a nuclear icebreaker, and provides a relatively detailed account of a successful attempt to penetrate a nuclear-weapon assembly facility in Sarov.[42] In striking contrast to most openly published accounts of similar exercises, the story acknowledges that the defense side lost. In some cases, tests involving stealth or deception rather than forceful attack are reportedly carried out without notice, so that the defenders do not realize that what is underway is a test.[43]

These kinds of tests mainly assess the physical-protection system. Assessing the performance of material control and accounting systems is always challenging. In Russia, there

---

[41] Voronov, "Terrorists in 'Nuclear Cities'."
[42] Voronov, "Terrorists in 'Nuclear Cities'."
[43] Ibid. Similarly, in 2003, one of the authors (Bunn) interviewed a former Russian military intelligence (GRU) officer who had led no-notice security exercises at major facilities such as power plants (both nuclear and non-nuclear). In these tests, the scenario typically involved deception – such as the adversaries using fake uniforms and identifications to gain access to facilities. Defenders did not know that a test was underway. Personal communication, October 2003.

are specified requirements for how accurate material accounting must be, what types of material controls must be used, and the like. For an integrated assessment of the overall system, a US–Russian project adapted a US-developed approach to assessing the actual effectiveness of MC&A systems and then piloted it at some Russian nuclear facilities, but it is not clear that this approach is being widely implemented.[44]

Consolidation

Nuclear security is never perfect. Every site with nuclear weapons, HEU, or separated plutonium represents another risk. Moreover, since securing each such site is costly, reducing the number of sites makes it possible to achieve higher levels of security at lower cost. Hence, consolidation is a key part of strengthening and sustaining nuclear security.[45]

Russia has consolidated its nuclear weapons and nuclear-material stocks substantially since the 1990s, cutting the number of locations where nuclear weapons exist, phasing out HEU or plutonium operations at several major sites, and reducing the number of buildings with HEU or plutonium at a number of sites.[46] It appears that all of Rosatom's defense nuclear activities are now to be carried out by a modest list of sites designated as Federal Nuclear Organizations.[47]

Nevertheless, Russia still has the world's largest numbers of nuclear-weapon storage locations and buildings with HEU or separated plutonium.[48] Russian officials confirm that while particular facilities may shut down for cost reasons, Russia has no specific plan for consolidating

---

[44] See A.S. Sviridov et al., "Application of MSET Method for Assessing Effectiveness of Nuclear Material Control and Accounting System at a Nuclear Facility," in *Proceedings of the 50th Annual Meeting of the Institute of Nuclear Materials Management, Tucson, Arizona, July 6-12* (Northbrook, Ill.: INMM, 2009), and A.S. Sviridov et al., "Results of Pilot Implementation of MC&A Effectiveness Tool (MSET-R) at Russian Facilities," in *Proceedings of the 53rd Annual Meeting of the Institute of Nuclear Materials Management, Orlando, Florida, July 15-19* (Northbrook, Ill.: INMM, 2012).

[45] For discussion, see . The communique of the last nuclear security summit in which Russia joined emphasized that nuclear material should be "secured, consolidated, and accounted for." See "The Hague Nuclear Security Summit Communiqué" (The Hague: Ministry of Foreign Affairs, the Netherlands, March 25, 2014), https://www.nss2014.com/sites/default/files/documents/the_hague_nuclear_security_summit_communique_final.pdf.

[46] Pavel Podvig, *Consolidating Fissile Materials in Russia's Nuclear Complex* (Princeton, N.J.: International Panel on Fissile Materials, May 2009), http://fissilematerials.org/library/rr07.pdf (accessed May 8, 2017).

[47] Office of the Russian President, "On Federal Nuclear Organizations," Decree No. 467, June 26, 2014.

[48] See, for example, *Securing the Bomb 2010,* p. 33. See also discussion in bunn and Harrell, *Consolidation.*

its huge complex of HEU-fueled research reactors or converting them to LEU.[49] Russia could achieve its civilian and military nuclear missions effectively at lower cost and risk by reducing the number of sites where its nuclear weapons and weapons-usable nuclear material exist.

US assistance helped with consolidation in Russia in several ways. First, Russian and US experts in the MPC&A program worked together to reduce the number of buildings at individual sites and establish secure centralized storage facilities at some sites. Second, the Material Consolidation and Conversion (MCC) effort provided funding to two Russian sites to receive HEU from other sites and blend it down to LEU, with some 17 tons of HEU blended in that effort by the time the program ended. Russian experts suggested that a number of buildings were being cleaned out in this effort, but the US side was only informed about one site where all HEU had been removed (the Krylov Shipbuilding Institute). Third, Russia and the United States worked together on feasibility studies for converting six Russian research reactors from HEU to LEU, and one of these reactors (the Argus reactor at Kurchatov) was actually converted. In addition, in the US–Russian HEU Purchase Agreement that was completed in 2013, Russia destroyed 500 metric tons of weapons-grade HEU, though it is not clear whether this led to completely removing HEU from any substantial number of buildings.

While US funding for such consolidation is no longer available, Russia continues with some consolidation on its own, such as the removal of weapons-grade uranium metal from the BFS critical assembly at the Institute for Physics and Power Engineering (IPPE) in Obninsk.[50] These efforts are largely driven by cost concerns, rather than efforts to strengthen security.

Unfortunately, Russian facility managers have little incentive to consolidate their nuclear material to fewer locations. Operators of research reactors often express concern that, without HEU or plutonium, their reactor would be less important and might no longer be successful in competing for funding. Russian physical-protection regulations do not offer much opportunity for reducing security costs by eliminating HEU or plutonium at sites; since sites have to protect against both nuclear material theft and facility sabotage, the rules that specify the security measures required based on the type of assets at a site often would require about the same security for a site whether it had weapons-usable material or not.[51] Russia has never considered

[49] Interview with Rosatom official, October 2015.
[50] Interview with Russian laboratory expert, July 2015.
[51] For example, see Bunn and Harrell, *Results of a Survey*, p. 31.

reducing the number of HEU or plutonium sites within its borders to be a priority, and with no plan for further consolidation, few incentives driving such consolidation, and cooperative consolidation efforts terminated, the prospects for substantial further consolidation do not look bright.

International cooperation

International cooperation, with the United States and with several other countries, has played a fundamental role in the dramatic improvements in Russian nuclear security. Both the Russian and US governments acknowledge the important role this cooperation played. Both, however, also acknowledge that the approaches that were appropriate in the 1990s are no longer appropriate today. This does not mean that a more equal form of cooperation would no longer be valuable—after all, the United States has nuclear-security cooperation with countries such as the United Kingdom and France. Unfortunately, however, with the current state of US-Russian relations, nuclear security cooperation remains largely in a deep freeze.

This lack of nuclear-security cooperation means that Russian approaches to nuclear security will evolve in isolation, separated from what other countries are doing, and with less external pressure for improvement. Russia's sites no longer get, in effect, international peer reviews, offering a different perspective on potential vulnerabilities and what might be done to reduce them, and there is less flow of new expertise and ideas. The lack of cooperation also means that there is no US funding available for nuclear-security efforts, but that is likely to be a more modest effect (given the low level US funding had already reached), except perhaps for a few activities that had become dependent on US funds. Finally, the current lack of cooperation is eroding personal relationships among technical experts that had proved extremely useful in building trust and finding new ways to overcome obstacles. Such relationships are likely to be crucial if cooperation begins again – or in the event of a nuclear security emergency.[52]

[52] See Siegried S. Hecker, ed., *Doomed to Cooperate: How American and Russian Scientists Joined Forces to Avert Some of the Greatest Post-Cold War Nuclear Dangers* (Los Alamos: Bathtub Row Press, 2016).

Adding it up: sustainability and continuous improvement

Given the strengths and weaknesses of each of these drivers of nuclear security, will Russia sustain and improve its nuclear-security systems over time? No one knows for sure. The discussion so far offers both reasons for optimism and reasons for doubt.

Concerned that the high-tech security systems it had helped install might *not* be sustained after foreign assistance phased out, the United States provided extensive assistance focused on sustainability. The US Department of Energy, working jointly with Rosatom, identified a set of seven sustainability criteria, ranging from having a focused MPC&A organization to conducting performance testing and operational monitoring of how the nuclear-security systems worked.[53]

Russian and American experts, unfortunately, never understood the concept of sustainability in the same way. In Russia, as a rule, "sustainability" refers to sustaining the equipment—keeping it operable, making repairs, keeping supplies of spare parts and consumables on hand, and replacing broken equipment. To many nuclear facilities, these equipment-focused tasks are their main sustainability role——in the past, to be done with US money as much as possible.

Americans, by contrast, interpret "sustainability" as sustaining a high level of nuclear-security performance over time, going well beyond equipment maintenance. This requires a set of management practices adapted to the specific MPC&A arrangements at each site. If Russians embraced this interpretation of the term, this could help eliminate existing gaps in sustainable nuclear security and facilitate effective use of available resources.

Although this difference in perception of sustainability is often obvious in the work on particular sustainability elements, US experts did not pay sufficient attention to developing a common understanding of the underlying concept and of the contribution of each individual element to overall sustainability. To achieve sustainability in this broader sense requires a combination of resources, incentives to use these resources to achieve nuclear-security goals, and organization to facilitate the use of these resources and other aspects of the system.[54]

---

[53] For discussion, see, for example, Victor V. Erastov and Charles Bolton, "Sustainability of MPC&A Systems Developed under U.S.–Russian Cooperation Program at Rosatom Sites and Organizations," in *Proceedings of the 47th Annual Meeting of the Institute of Nuclear Materials Management, Nashville, Tenn., July 16-20* (Northbrook, Ill.: INMM, 2006).

[54] For an early version of this formulation, see Oleg Bukharin, Matthew Bunn, and Kenneth N. Luongo, *Renewing the Partnership: Recommendations for Accelerated Action to Secure Nuclear Material in the Former Soviet Union*

In short, while Russia has established most of the elements necessary for sustainable nuclear security, there are still significant uncertainties clouding the picture. Resources are likely to be constrained, with ongoing pressure to cut costs and increase profits; existing nuclear-security regulations and requirements create incentives to maintain nuclear-security systems, but there are still questions as to how effective these regulations are, and how much site leadership and security culture will drive sustainability; and, while key organizations needed for sustainability are in place, regulatory organizations in particular still have limited power and resources.

Four scenarios for the evolution of nuclear security in Russia

Taking these factors into account, how might nuclear security in Russia evolve in the future? The answer is highly uncertain. We have identified four broad classes of potential scenarios, listed here in declining order of the level of nuclear security that would result:

- Continuous improvement;
- Stasis;
- Slow erosion;
- Collapse.

Below, we describe the characteristics each scenario might have; what factors might push Russia's nuclear-security system in that direction; and observable indicators that would suggest that a particular scenario was evolving.[55] As both good and bad changes in nuclear security are often underreported, it will take close examination of publicly available information to identify shifts from the "stasis" scenario.

For the past two decades, nuclear security in Russia has clearly been on a "continuous improvement" track. Now, however, while there are improvements being made at some locations, the most likely trajectories appear to be on the "stasis" or "slow erosion" paths. There

(Washington, D.C.: Russian American Nuclear Security Advisory Council, 2000), http://belfercenter.ksg.harvard.edu/files/mpca2000.pdf.

[55] Because different elements of the nuclear security system interact, some factors discussed below – such as strong security cultures and effective performance testing – are both potential causes of improvement and potential results of other causes.

is still a chance to move onto a long-term continuous improvement track, and we offer some recommendations to increase the chance of that outcome in the conclusions section. But there is also at least a modest chance of moving in the direction of system collapse, particularly if Russia were to head back toward systemic political and economic crises.

Continuous improvement

Characteristics. In a continuous-improvement scenario, each of the six drivers assessed earlier in this paper would be in place and functioning well. There would be ongoing steps to improve the performance of nuclear-security and accounting systems and identify and address potential vulnerabilities. In such a scenario, nuclear sites would have available, and would allocate, the funding needed to sustain and to strengthen security and accounting equipment, operations, and training programs.

This scenario would include a clear focus on achieving a strong security culture at Russian nuclear sites, with widespread belief in the threat, understanding of the importance of security and accounting systems to address it, and a questioning attitude focused on finding and fixing vulnerabilities. Because of that culture, sites and regulators would be working with some degree of collaboration to find and address gaps or issues in nuclear security regulations, and regulators would have effective programs in place to ensure full compliance.

Drivers. What factors might drive Russia's nuclear-security system toward a continuous-improvement scenario? In a 2012 Harvard survey, nuclear-security experts from many countries reported that major incidents were the most important factor that had driven steps to strengthen nuclear security in their countries.[56]

But for incidents to result in real and lasting change requires government leaders to prioritize nuclear security. The emergence of such nuclear-security champions in positions of power would be another key factor that could lead to continuous improvement. More broadly, the leadership commitment, threat perception, and strong security cultures described earlier in this article would be both drivers of and results of a continuous improvement scenario.

Incidents are not the only factors that can drive change. Effective vulnerability assessment and realistic testing programs can help motivate government officials and site

[56] Bunn and Harrell, *Results of a Survey*.

leaders.[57] In the United States, for example, repeated failures in "force-on-force" exercises helped convince government leaders that funding for more stringent nuclear-security measures was needed. In Russia, early in President Putin's tenure, press reports indicated that a failed security test at a nuclear site led him to call in the minister of atomic energy on a weekend to demand security improvements.[58]

Should Russia choose to renew nuclear-security cooperation with other countries (including the United States), or to initiate broader cooperation with the IAEA within Russia, this could be another driver of continuous improvement, offering additional ideas and motivation for addressing particular gaps. Often gaps are not perceived by those who have been living with them for years, but a fresh set of eyes bringing experience of different ways things are done elsewhere can point out potential vulnerabilities and suggest solutions.

Finally, the nuclear industry itself could become a driver of continuous improvement. Countries exporting nuclear reactors have long understood that their reactors' reputation for safety is crucial to their ability to make sales abroad. Should the Russian nuclear sector conclude that a strong security reputation would help their commercial endeavors, it could drive additional focus and attention on nuclear security. The small industry of companies providing equipment and expertise in nuclear security and accounting may also be able to push for additional use of their products and services over time.

Observable indicators.

- Sites reporting implementation of new nuclear security and accounting initiatives;
- Reports of major nuclear security-related procurements;
- Reports of new testing, assessment, and security culture programs;
- New high-level policy documents and legislation acknowledging the threats and identifying steps to address them;

---

[57] Bunn and Harrell, *Results of a Survey*, p. 28.
[58] See, for example, "The Ministry of Atomic Energy in the Middle of a Scandal," trans. BBC Monitoring Service, *Nezavisamaya Gazeta*, December 14, 2001; Yuri Golotyuk, "Peaceful Atom Preparing for War," *Vremya Novostei*, November 12, 2001.

- Reports of "federal targeted programs" for nuclear-security improvements with substantial funding;
- Reports of changes in rules and procedures that address particular identified gaps;
- Nuclear-security improvement trends identified in Rostechnadzor annual reports;
- Renewed Russian interest in international cooperation, with Russian experts offering sophisticated ideas about ways to address particular issues and detailed questions about common implementation challenges.

Stasis

Characteristics. As the name implies, a stasis scenario would be characterized by little or very slow change in current nuclear-security approaches in Russia. Nuclear security and accounting systems would neither decline substantially nor improve substantially over time. As we envision it, however, the "stasis" scenario would not mean that all the physical protection and material accounting and control systems would remain exactly as they are today. Existing Russian physical-protection rules require that nuclear operators regularly assess the effectiveness of their systems against the existing threats as they continue to evolve and adjust their systems as needed, and this would continue to be the case in the "stasis" scenario. In general, in today's approach in Russia, this does not often lead to major investments in new security systems, but it might lead to adding more guards at a particular part of a site, changing access control arrangements, modifying guard force tactics, or other steps with relatively modest costs.

Thus, in the stasis scenario, there would be some effort to adapt to evolving adversary threats, but the changes would generally be quite limited. There would be little focus on adapting to changing technologies, or on discovering and addressing previously unknown vulnerabilities. In this scenario, the Russian government and the organizations managing Russian nuclear sites would provide the funding necessary to sustain the most needed security and accounting equipment, operations, and training programs, but little or no funding would be available for substantial improvements. Nuclear security and accounting rules and procedures would continue to be revised from time to time, but the changes would be modest and the quality of their implementation would remain roughly as it is today, as would the level of security culture among the staff in Russian nuclear organizations.

Drivers. The stasis pathway would most likely be driven foremost by the absence of any clear reason to improve. The complacent view that existing nuclear-security arrangements are sufficient (or perhaps excessive) is widespread among nuclear officials in Russia (and in most other nuclear countries). If there are no major theft or sabotage attempts, institutions are likely to conclude that the existing security measures are sufficient to the task, and there will be little pressure to change them.

Institutional lock-in could be another key driver of a stasis scenario. Once security rules and procedures are in place, making the case for weakening or strengthening them requires officials to admit that previous decisions were wrong (either leaving too much risk or imposing too much cost and inconvenience), and to accept responsibility for the costs of strengthened regulations or the increased risks of weakened ones.

Observable Indicators.

- The absence of reports of changes in security and accounting rules or procedures (though such an absence could also result from simple lack of transparency).
- On the one hand, experts at sites reporting that they could not get funding for proposed new nuclear-security projects; on the other hand, the absence of similar reports of inadequate funding for existing nuclear-security programs (or of reports of other issues leading to the decline of existing security programs).
- Reports from regulatory agencies on detected violations showing no clear trend of either increasing or decreasing frequency or severity (and most of the violations being relatively minor).

Slow Erosion

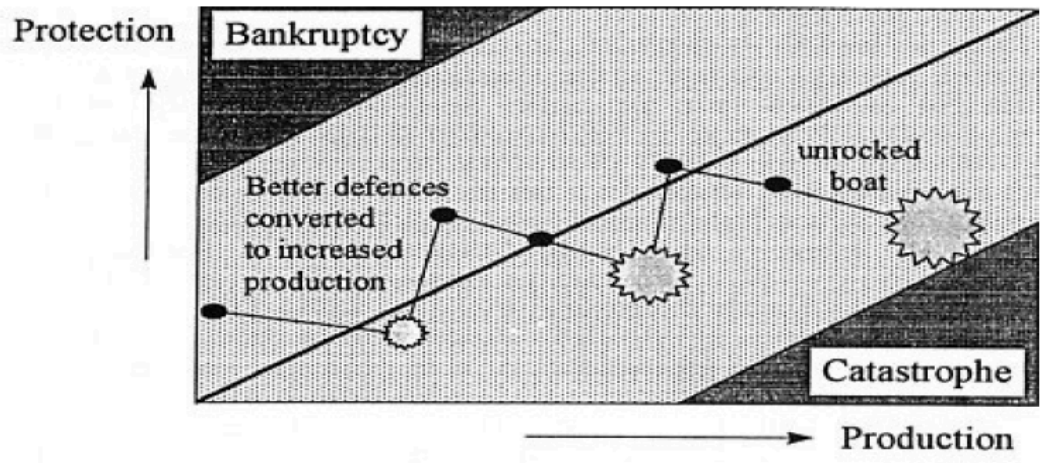
Characteristics. Fundamentally, the slow-erosion scenario would be characterized by a decline in nuclear-security performance over time. This would include inadequate funding to sustain some aspects of nuclear security and accounting equipment, operations, regulation, and training programs. Nuclear-security regulation might weaken over time, for example with regulatory agencies granting increasing numbers of exceptions to rules. In this scenario, most of the drivers of effective nuclear security would likely be weak or absent: there might be weak leadership commitment and security culture at many Russian nuclear sites; little if any international cooperation offering outside views on what could or should be done; little focus on creative and in-depth vulnerability assessment or realistic testing of security performance; weak regulatory oversight; and little effort to consolidate nuclear material.

Drivers. The most important drivers of a slow-erosion scenario would be weak security culture and growing complacency about the threat and the adequacy of even modest security measures to cope with it, combined with pressures to allocate funds and attention elsewhere. When there has been a long period without any substantial incidents, it becomes possible to make the case that certain requirements can safely be relaxed, and budget and production pressures to do so are ever-present.

Figure 1, from author James Reason, illustrates the point as it applies to safety.[59] He envisions an organization starting off with some balance between spending on production (too little of which will lead to bankruptcy) and spending on protection (too little of which will lead to catastrophe). As time passes without major incidents, complacency will set in, people in the organization will want to cut corners on protection to get more production, and the system will drift toward less protection. Then an incident will drive it back toward protection. Paradoxically, having no incidents for an extended period can lead to catastrophe, as nothing pushes the system back toward protection.

Figure 1: Navigating between protection and production

[59] James Reason, *Managing the Risks of Organizational Accidents* (Aldershot, UK: Ashgate, 1997), p. 5.



Diane Vaughan has outlined a similar phenomenon in what she calls the slow "normalization of deviance," as circumstances that differ from what had previously been required become accepted and routine over time.[60] She identifies three key underlying drivers that determine whether organizations will deviate from their intended course: competitive resource pressures that create incentives to cut corners; structures and processes within the organization; and the organization's regulatory environment.[61]

The phenomenon of the "unrocked boat" is a particular problem for sustaining effective nuclear-security measures, because genuine incidents happen so rarely (and so little information about them is circulated when they do occur, leaving many officials and managers unaware of them). In most countries, no serious attempt to steal HEU or separated plutonium, or to sabotage a nuclear facility, has ever occurred. For most guards at nuclear facilities, 100 percent of the alarms they respond to in their entire careers will be false alarms or exercises. Norman Augustine has described the guards' situation—trying to stay constantly on alert for something that never happens, in the presence of constant false alarms—as "an endeavor of chilling monotony… a mind-numbing challenge."[62]

Resource pressures would likely be a critical driver of a slow-erosion scenario. In an environment in which the nuclear industry was under pressure to generate profits and receiving

---

[60] Diane Vaughan, *The Challenger Launch Decision: Risky Technology, Culture, and Deviance at NASA* (Chicago: University of Chicago Press, 1996).
[61] Vaughan, *The Challenger Launch Decision*, p. 458.
[62] Norman Augustine, "Letter to Secretary of Energy Steven Chu" (Washington D.C.: December 6, 2012), http://pogoarchives.org/m/nss/20121210-augustine-ltr.pdf.

less support from the Russian federal government, the incentive to cut back on investments in security would be strong.

If the group of officials and managers seeking to reduce the costs and inconveniences of security were stronger and had more influence on policy than nuclear-security advocates, this could be another driver of a slow-erosion scenario. Rosatom's intense focus on either profit or the nuclear-weapons program already creates a situation in which those officials focused on ensuring security may get less attention from senior decision-makers than others.

Observable indicators.

- Site experts reporting inadequate funding for security programs;
- Reported cases of significant security weaknesses – e.g., inadequately maintained fences and barriers, cutbacks in or poor training and pay for guard forces, and more;
- Regular reports of detection of significant violations of nuclear security and accounting rules, or of decisions to weaken security and accounting rules or allow major deviations from them.

All of these indicators were frequent in Russia in the 1990s, and some continued into the 2000s.

Collapse

Characteristics. Finally, one cannot rule out a drastic collapse of the nuclear security system—as occurred with the collapse of the Soviet Union. If Russia again suffered severe political, economic, and social crises, this could lead to major nuclear-security cutbacks. A collapse scenario might be characterized by widespread failures to maintain nuclear security and accounting systems; drastic reductions in nuclear-security funding: inadequate funding for the Russian regulators to do their jobs; and possibly large-scale unemployment, salary cutbacks, or salary delays at major nuclear facilities. There would likely be a complete absence of the major drivers of nuclear security described earlier in this article.

Drivers. The drivers of a collapse scenario would be systemic political and economic crises in Russia. These might include major deficits in the Russian government budget and the budgets of nuclear facilities, with pressure to focus remaining resources on generating profits. Here, too, complacency—putting nuclear security far below more urgent items on the list of areas to be addressed—would likely be a major driver.

Observable indicators.

- Major crises affecting the society in general and the nuclear sector in particular;
- Cases of drastic budget cuts at nuclear facilities, and much reduced or unpaid staff salaries;
- Widespread reports of nuclear-security and accounting systems that were not being maintained;
- Many reports of regulators finding major violations, or of regulators being unable to do their jobs.
- Actual successful or attempted nuclear thefts or sabotages of nuclear facilities.[63]

Assessing the scenarios

Clearly, the continuous-improvement scenario would best serve Russian, US, and world security interests. At present, however, we believe that over the next five to ten years, unless major new

[63] Although such events could occur in any scenario, the probability would be progressively higher in each scenario than in the previous one. Their probability would be much higher under the collapse scenario.

steps are taken, the stasis and slow-erosion scenarios are most likely. Russian nuclear security over the past three years has been in the stasis mode, though some modest improvements are being made in some areas. A major effort would be needed to reach the continuous-improvement path. The collapse path would only be likely in the context of large-scale crises.

Steps to maximize the chances of continuous improvement

The future of nuclear security in Russia depends primarily on the Russian government's own decisions. The best opportunity for putting Russian nuclear security on the path to continuous improvement is for the Russian government to take action in each of the key areas described in this article.[64]

Given the importance of belief in the threat to a strong security culture, one important initiative would be to ensure nuclear officials and managers have more detailed threat information, including information about real incidents and the lessons learned from them. Much like programs for operational experience and lessons learned in nuclear safety, Russia could establish a program to collect and analyze incident data—from incidents at nuclear sites in Russia and elsewhere, and from non-nuclear incidents (such as major thefts from guarded facilities) that also provide insight into plausible adversary capabilities and approaches.[65] Showing nuclear managers how their sites might be vulnerable to capabilities and tactics adversaries have already used in real incidents can be a powerful motivator.

Another important initiative would be for Russia to more frequently carry out realistic tests of the real performance of nuclear-security systems against adversaries trying to overcome them, including force-on-force exercises. Combined with in-depth effectiveness evaluation by creative teams with incentives to find vulnerabilities and suggest proposed fixes, these could highlight remaining vulnerabilities and motivate sites to address them.

Renewed international cooperation would be another important step. Both Russian President Putin and US President Donald Trump have called for expanding US–Russian cooperation in areas where the countries have common interests. Cooperation could focus on

[64] For recommendations on increasing the chance that all countries with nuclear weapons, HEU, or separated plutonium on their soil will move onto such a path, see Bunn et al., *Preventing Nuclear Terrorism*, pp. 96-132.
[65] See discussion in .

exchanges of ideas among experts about common challenges and best practices, based on principles of equality, mutual respect, protection of sovereignty, and protection of necessary secrets. Such discussions can bring fresh sets of eyes and of ideas to help strengthen nuclear security.[66]

Despite the major grievances both the Russian and US governments have against the other, both countries have strong national interests in ensuring that their nuclear stockpiles and complexes are safe and secure. Nevertheless, a renewal of nuclear-security cooperation, however much it would serve both sides' interests, is only likely in the context of declining political conflicts, and perhaps as part of a package that included items of interest to Russia such as nuclear-energy cooperation and nuclear-science cooperation as well. Dialogue between technical experts can help provide new solutions and build new bridges, helping the governments overcome the obstacles to cooperation.

The United States, in particular, should continue reaching out to Russian experts with ideas about best practices and steps that could be taken, regardless of whether the Russian side is willing to respond or engage. In some cases, Russian experts have been willing to use US expertise, even where they were hesitant to pursue genuinely joint work due to information sensitivity.

Beyond the United States, Russia should take a broader approach to nuclear-security cooperation, including supporting nuclear security in developing countries (an area where, in some cases, the United States and Russia might work together), and with developed countries with which Russia has a better relationship (such as Germany). To avoid having the international nuclear-security dialogue become too US-driven, Russia should participate more actively in supporting the IAEA's nuclear-security work, making larger contributions of both money and expertise, and join the strengthening nuclear-security implementation initiative (INFCIRC/869), rather than leaving Russia isolated as the only non-participant among the permanent five members of the Security Council. Russia might also consider establishing a nuclear-security

---

[66] For a recent report outlining ideas in this area, see *Pathways to Cooperation: A Menu of Potential US–Russian Cooperative Projects in the Nuclear Sphere* (Washington, D.C.: Nuclear Threat Initiative and Center for Energy and Security Studies, February 2017), http://www.nti.org/media/documents/Pathways_to_Cooperation_FINAL.pdf (accessed May 8, 2017). The authors were the U.S. and Russian experts providing input papers on nuclear security for that report with more detailed suggestions, available on request.

working group in the Global Initiative—a forum more conducive to Russian influence, since Russia is co-chair. Participation by both US and Russian experts in working groups at the IAEA and the Global Initiative can keep at least a few relationships alive – but working through such groupings is inevitably more limited in what can be accomplished than direct cooperation.

Even if major US–Russian geopolitical disagreements cannot immediately be resolved, the United States should be willing to re-engage in a package of cooperation including nuclear energy, nuclear security, and nuclear science. It is overwhelmingly in the interests of the United States, Russia, and the world, for the experts managing the world's two largest nuclear stockpiles to be talking to each other and cooperating to manage those stocks safely and securely.