NUCLEAR SECURITY CULTURE: THE CASE OF RUSSIA

Center for International Trade and Security
The University of Georgia

NUCLEAR SECURITY CULTURE: THE CASE OF RUSSIA

University of Georgia
December 2004

ABOUT THE CENTER FOR INTERNATIONAL TRADE AND SECURITY

The Center for International Trade and Security (CITS) works to address the dangers posed by transfers of weapons of mass destruction (WMD) and WMD-related technology and materials. CITS seeks to accomplish its mission by:

- Engaging and informing policymakers, industry representatives, educators, and the public, both in the United States and abroad, about dangers stemming from the trade in and theft of weapons and weapons components. CITS communicates these concepts through policy research, public forums, editorials, briefings, Internet publications, and the publication of a journal, *The Monitor: International Perspectives on Nonproliferation*
- Facilitating international dialogue through exchanges of officials and experts that will promote greater cooperation in preventing the spread of dangerous weapons and technology
- Establishing training programs for government officials and others in "best practices" for controlling, monitoring, and preventing the trade in WMD and related items
- Preparing future leaders for careers in international security and nonproliferation

The CITS Security Policy Program is focused on:

- Improving understanding and awareness of the importance of training and motivating personnel responsible for protecting nuclear and other WMD-related materials
- Promoting U.S.-Russian dialogue on nonproliferation and threat reduction
- Facilitating U.S. assistance to Russia and the other former Soviet states through analysis of their nuclear and military-industrial complexes
- Analyzing and strengthening security at WMD-related facilities internationally

Center for International Trade and Security
120 Holmes/Hunter Academic Building
University of Georgia
Athens, GA 30602

Dr. Gary K. Bertsch, *Director*

Dr. Michael D. Beck, *Executive Director*

(706) 542-2985

fax (706) 542-2975

cits@uga.edu

http://www.uga.edu/cits

NUCLEAR SECURITY CULTURE: THE CASE OF RUSSIA

EDITORS

Igor Khripunov and James Holmes

CO-AUTHORS

Igor Khripunov

Dmitriy Nikonov

Maria Katsva

This report has been supported in part with funds from the Nuclear Threat Initiative, the North Atlantic Treaty Organization, and the University of Georgia. Its contents represent the views, findings, and opinions of the authors, and are not necessarily those of the supporting organizations.

Acknowledgments

This report has been reviewed in draft form by individuals chosen for their perspectives and technical expertise. Specifically, the authors and editors would like to express their gratitude to:

Peer Reviewers:

- Michael Beck (Center for International Trade and Security)
- Allen Blancett (Independent expert, USA)
- Matthew Bunn (Harvard University/Belfer Center)
- Christopher Eldridge (U.S. National Academies)
- Irina Kupriyanova (Institute of Physics and Power Engineering, Russia)
- William Potter (Center for Nonproliferation Studies)
- Yuri Volodin (Federal Service for Ecological, Technical, and Nuclear Oversight, Russia)

Although the reviewers listed above provided many constructive comments and suggestions, they were not asked to endorse the content of the report, nor did they see the final draft before its release.

In addition, Charles Packer (Cherrystone Management Inc., Canada) and Paul Ebel (BE Inc., USA) contributed to Chapter I; Nikolay Ischenko, Rector, and Vladimir Kornelyuk, Head of Department at the Moscow Institute for Professional Training "Atomenergo," participated in the development of Appendix II; and Jessica Howard (CITS) helped design and lay out the final publication.

About the Project Team

Igor Khripunov is the associate director of the Center for International Trade and Security and an adjunct professor at the University of Georgia School of Public and International Affairs. Dr. Khripunov served for six years as an international civil servant at the UN Secretariat in New York before joining the USSR Ministry of Foreign Affairs in 1977. In 1983, he received a Ph.D. in international relations from the Moscow-based Diplomatic Academy and resumed his diplomatic career as an arms control expert. He has served at the University of Georgia since 1992.

James Holmes is a senior research associate at the Center. He edits the Center's journal, *The Monitor*. A former U.S. Navy officer, Dr. Holmes served on board the battleship USS *Wisconsin*, taught engineering at the Surface Warfare Officers School Command, and served as professor of strategy at the U.S. Naval War College. He is a graduate of Vanderbilt University, Salve Regina University, the Naval War College, Providence College, and the Fletcher School of Law and Diplomacy at Tufts University.

Dmitriy Nikonov is a senior research associate at the Center. He has been affiliated with the Center since 1995. Dr. Nikonov received a B.A. from the Pyatigorsk State Institute of Foreign Languages in Russia, an M.A. from Western Illinois University, and a Ph.D. from the University of Georgia.

Maria Katsva is a research associate at the Center. Ms. Katsva graduated from Moscow State University and earned an M.P.A. from the University of Georgia. Before coming to UGA, she served as a research associate at the Moscow-based Center for Policy Studies in Russia.

Contents

List of Abbreviations

CIA	Central Intelligence Agency (U.S.)
CTR	Cooperative Threat Reduction Program (Nunn-Lugar Program)
DBT	Design Basis Threat
DOE	Department of Energy (U.S.)
FIS	Federal Information System (Russia)
FSB	Federal Security Service (Russia)
GAN (Gosatomnadzor)	Federal Nuclear and Radiation Oversight Agency (Russia)
GAO	General Accounting Office (U.S.)
IAEA	International Atomic Energy Agency
INFCIRC	Information Circular (IAEA)
IPPAS	International Physical Protection Advisory Service (IAEA)
KGB	State Security Committee (USSR)
LANL	Los Alamos National Laboratory (U.S.)
MC&A	Material Control and Accounting
Minatom	Ministry of Atomic Energy (Russia)
MOD	Ministry of Defense (Russia)
MPC&A	Material Protection, Control, and Accounting
MVD	Interior Ministry (Russia)
NKVD	People's Commissariat for Internal Affairs (USSR)
NSC	National Security Council (U.S.)
PPS	Physical Protection System
Rosatom	Federal Atomic Energy Agency (Russia)
Rostekhnadzor	Service for Environmental, Technological, and Nuclear Oversight (Russia)
VA	Vulnerability Analysis
WMD	Weapons of Mass Destruction

PREFACE

This report on *Nuclear Security Culture: The Case of Russia* probes an obvious, yet often overlooked dimension of security: the human dimension. It examines security measures at facilities in Russia's civilian nuclear sector and finds that, after over a decade of U.S. and European security assistance, security unfortunately remains porous. Why? In 1991 the U.S. government, under the visionary leadership of Sen. Sam Nunn (D-GA) and Sen. Dick Lugar (R-IN), created the Nunn-Lugar Cooperative Threat Reduction Program to help Russia safeguard its inventory of nuclear weapons, fissile materials, and the associated technology. The Nunn-Lugar Program and other initiatives such as the G-8 Global Partnership Against the Spread of Weapons and Materials of Mass Destruction have furnished Moscow with a panoply of high-tech surveillance systems, alarms, and other equipment, as well as low-tech but crucial items such as security fences.

Even so, lapses in security have persisted. Hardware by itself does not produce security; people do. Recognizing this, the U.S. Department of Energy (DOE) has put considerable effort into modifying the security culture, both here in the United States and in Russia's civilian nuclear complex. But cultures are stubborn things. Indeed, when I took over responsibility for security at the Department of Energy in 1999, I was disturbed by the lackadaisical attitudes displayed by some DOE employees entrusted with safeguarding classified information. It is clearly apparent, based on recent security lapses at DOE facilities, that much more work must be done to change that internal culture. Thus, it comes as no surprise that reshaping the security culture at Russian sites has proved to be a difficult undertaking. Cultural change clearly involves far more than building a fence or installing an alarm.

The actions of people are shaped by their national culture and the culture of the organization in which they work. This report investigates how Russia's painful transition to market democracy, the legacy of communist and tsarist rule, and budgetary considerations continue to work against nuclear security. Federal budgets fell off sharply in the aftermath of the Cold War. The nuclear sector was particularly hard hit during this time of austerity. Managers were forced to seek out foreign contracts in an effort to keep their facilities afloat. Workers saw their salaries slashed and found it nearly impossible to provide for their families. There were documented cases when employees at various levels of the nuclear hierarchy were tempted to divert fissile materials from their facilities, despite the damage this illicit activity would do to national security.

Recent events have brought the problem of security culture into sharp focus. Improving security culture should be a key ingredient in a multifaceted response to terrorist acts such as the ones that shook Russia in August-September 2004. Like September 11, 2001, these attacks served notice that the new breed of terrorists would strike at Russia or the West with whatever means available–including nuclear weapons or "dirty" bombs. They will seek out fissile materials from sites where security is lax or insiders can be co-opted. An efficacious security culture impels employees not only to execute preexisting procedures but to innovate when that kind of unforeseen circumstance arises–as it undoubtedly will, given the limits on policymakers' ability to predict the future.

This report examines all of these factors, and more, before deriving a set of specific recommendations that will help policymakers in Russia and the West reach wise policy decisions about nuclear security. It is fitting that the University of Georgia Center for International Trade and Security and the Nuclear Threat Initiative undertook such an assessment. The report draws on the years of experience amassed by the Center, which began building ties in the Russian nuclear sector immediately after the fall of the Soviet Union. It benefited from the generous support of the

Nuclear Threat Initiative, a charitable organization that "seeks to raise public awareness, serve as a catalyst for new thinking and take direct action" to reduce the spread of nuclear, biological, and chemical weapons, and thus the likelihood that these weapons will be turned against America and its friends.

While the report focuses on Russia, in large part because of the danger posed by that country's massive inventory of loosely guarded fissile materials, its findings apply equally to any country suffering from a deficient security culture. As a result, I am confident that the report will be of immediate and practical use to Russia while providing enduring lessons for policymakers elsewhere in the world. ■

EUGENE E. HABIGER
General, U.S. Air Force (Ret.)
Distinguished Fellow
Center for International Trade and Security
University of Georgia

INTRODUCTION

In December 2002, a few days before Christmas, suicide bombers leveled the government compound in the Chechen capital of Grozny, reputedly the most heavily guarded facility in the war-torn region. The blast killed 72 people and wounded another 210. The attackers drove a pair of trucks into the compound and set off two explosions with a combined force equivalent to a half-ton of TNT. The trucks passed through at least three supposedly airtight security checkpoints manned by interior troops. The intruders wore Russian military uniforms, flashed military IDs, and displayed forged passes on their windshields. The guards, who were presumably aware of the Chechens' threats to target key government officials, nonetheless failed to carry out their primary duty.

President Vladimir Putin's envoy in the region publicly faulted the interior troops, from the lowliest security guard to the most senior general, for dereliction of duty and a failure of accountability. Put another way, the lapse in security at Grozny stemmed from a breakdown of the "human factor" within the security force.

The concept of the human factor originated with a simple insight: that the best equipment in the world is no better than its operator. Nor can the best written directives in the world compensate for apathy or technical incompetence in the workforce. A vehicle to improve the human factor is "security culture," a concept that encompasses a set of managerial, organizational, and other arrangements. Security culture connotes not only the technical proficiency of the people entrusted with security, but also their willingness and motivation to follow established procedures, comply with regulations, and take the initiative when unforeseen circumstances arise.[1]

The Grozny incident has a peculiar resonance for this report. Troops from the Interior Ministry, the same government body designated to maintain security at Grozny, are assigned by law to protect Russia's nuclear sites. This alone should give us pause. Even more worrisome, similar failures of the human factor have been widely observed among nuclear site personnel. Breaches of security have been the eventual result in many of these cases.

The string of terror attacks in August-September 2004 and the subsequent dispatch of additional troops to reinforce security at nuclear sites only underscored the gravity of the situation. The Beslan hostage situation in September 2004 led to more intensive soul searching and self-evaluation, with implications for nuclear security. Observers tended to fault not only the seemingly omnipotent international terrorist network operating within Russia, but also "Russia's own complacency, uncoordinated action, lack of coherent organization and often criminal dereliction of duty for law enforcement officials at all levels."[2]

The importance of security culture is not confined to Russia. While security hardware and technical upgrades are critically important, the efficient use of machinery depends largely on the extent to which site personnel are not only trained to a high degree of technical proficiency, but also willing and motivated to perform their duties. Indeed, Gen. Eugene Habiger, a former "security

---

1. A useful definition of culture can be found in Edgar H. Schein, *Organizational Culture and Leadership*, 3d ed. (San Francisco, CA: Jossey-Bass, 2004), p. 47. This formal definition states that culture is "a pattern of shared basic assumptions that the group learned as it solved its problems of external adaptation and internal integration, that has worked well enough to be considered valid and, therefore, to be taught to new members as the correct way to perceive, think, and feel in relation to those problems."

2. Nikolay Ulyanov, "A Secret War Against Invisible Enemy with Classified Results," Strana.ru, September 1, 2004, <http://www.strana.ru/text/stories>.

czar" at the U.S. Department of Energy's (DOE) nuclear-weapons complex and a former commander of U.S. strategic nuclear forces, has observed that "good security is 20 percent equipment and 80 percent people."[3]

Evidence suggests that the security culture at Russian nuclear sites cannot cope with the nature and magnitude of modern threats. Poor management and motivation are largely to blame for this state of affairs. Personnel often fail to recognize how important it is to follow all procedures to the letter and to use the systems available for protecting nuclear materials. For example, foreign visitors note that Russian security personnel often make "exceptions" to security procedures in order to speed up the process of granting access to secure areas. Even when modern surveillance and alarm systems have been installed at Russian facilities, the equipment is rendered useless when the staff shuts off the power supply to reduce electricity bills. Reports also indicate that guards are in the habit of deactivating security and monitoring systems when they lose patience with false alarms.[4] Unless these shortcomings in Russia's security culture are directly and comprehensively addressed, some $2 billion in Western-funded security upgrades will fail to close the gaps in Russian nuclear security.

The root of the problem is that, for over a decade now, Russia has been undergoing a painful transition from an authoritarian system that dealt with security problems in its own heavy-handed way to a society with new values, career requirements, and human ambitions. Many government leaders and managers at Russian nuclear facilities doubt the efficacy of investing scarce funds in security upgrades and modernization. They have other priorities. Crime, corruption, the nation's still-immature legal order, and the prevailing pattern of indifference to law among the populace only worsen matters. Economic transition further exacerbates conditions. If a knowledgeable, adequately motivated workforce is the key to nuclear security, as we claim, then Russia clearly has a long way to go.

The requirements for security improvements in Russia are daunting. Installations housing an estimated 260 tons of weapons-usable fissile material have received either comprehensive or rapid security upgrades. However, the remaining 340 tons have not been adequately secured, while 70 sites housing nuclear warheads need more protection.[5] The past decade has witnessed numerous successful and attempted diversions of nuclear materials from Russian nuclear facilities. The increasing threat of terrorism adds to the urgency and seriousness of the problem. In February 2004, testifying before Congress about the global threat environment, CIA Director George Tenet warned that al Qaeda "continue[d] to pursue its strategic goal of obtaining a nuclear capability." Tenet stressed that "more than two dozen other terrorist groups [were] pursuing CBRN (chemical, biological, radiological, and nuclear) materials."[6] Russia, where these materials are available in great quantities, could well furnish al Qaeda and its brethren in Chechnya with components of mass destruction.

Echoing this warning, the National Commission on Terrorist Attacks Upon the United States, or 9/11 Commission, concluded in its final report that the danger of catastrophic attack within the United States would remain real as long as the world's most dangerous terrorists could

---

3. Matthew Bunn and Anthony Wier, *Securing the Bomb: An Agenda for Action* (Cambridge, MA: Belfer Center for Science and International Affairs, Harvard University, May 2004), p. 50, <http://bcsia.ksg.harvard.edu/BCSIA_content/documents/securing_the_bomb.pdf>.

4. U.S. General Accounting Office, *Security of Russia's Nuclear Materials*, GAO-01-312 (Washington, DC: Government Publishing Office, 2001).

5. Sen. Richard Lugar, "Persistent Diplomacy Needed for Nonproliferation Advances," Address to the National Press Club, Washington, DC, August 11, 2004.

6. George Tenet, "The Worldwide Threat 2004: Challenges in a Changing Global Context," Testimony before the Senate Select Committee on Intelligence, February 24, 2004.

acquire the world's most dangerous weapons. The commission emphasized that the government's main instrument to counteract theft or diversion at Russian sites, the Nunn-Lugar Cooperative Threat Reduction Program, was "now in need of expansion, improvement and resources." The commissioners urged the United States to "do all it can," provided "Russia and other countries do their part" as well.[7]

The U.S. Department of Energy seems to grasp the need for motivated nuclear personnel. Under a program designed to help Russia improve its material protection, control, and accounting (MPC&A) hardware and procedures, DOE explicitly acknowledges that a healthy security culture must be developed before Russia can take over sole responsibility for MPC&A. To that end, DOE defines security culture, the objective it has been working to achieve in Russia, as a set of attitudes, behaviors, organizational structures, and procedures that contribute to effective MPC&A operations.

According to the DOE definition, an effective MPC&A security culture consists of site and headquarters staff who understand the importance of MPC&A; MPC&A procedures that are promulgated, effective, and followed; a performance testing program that continuously assesses and improves the system; a system that identifies and reinforces best practices; and a system that reports problems and takes action to correct deficiencies.[8] For any major assistance program to succeed, however, it is necessary to factor in differences in national culture and psychology. The human and personal dimension of nuclear security is even more important in Russia than in Western societies because of Russia's distinctive history and national mentality, not to mention its ongoing, tumultuous post-Soviet transition.[9]

Though it has yet to be rigorously defined and internationally approved as a concept, security culture has become a common buzzword in nonproliferation and nuclear security circles. Different authors have been offering their own distinct visions of this concept,[10] but the common message seems to be the following: Effective nuclear security regimes depend not only on the design, quality, and condition of the equipment, but on the design and quality of administrative processes and on the behaviors of the people involved. Hence, a well-designed system can be degraded if the procedures necessary to operate and maintain it are deficient. It can also be degraded if the people assigned to assure security fail to follow procedures or fail to notice and report unusual occurrences. In other words, the entire nuclear security regime stands or falls by the people involved. It is this insight which prompted us to investigate the concept of nuclear security culture.

Accordingly, two major objectives of the report are to contribute to the ongoing debate over the meaning of nuclear security culture and to suggest a comprehensive model for building such a culture within an organization. Why Russia? We chose the case of Russia, first of all, because it

---

7. Thomas Kean et al., *Final Report of the National Commission on Terrorist Attacks Upon the United States* (New York: W. W. Norton & Company, 2004), pp. 380-381.

8. Charles Bolton, Lorilee Brownell, and William Toth, "The Department of Energy's Approach to Sustainability," Paper Presented at the 45th Annual Meeting of the Institute for Nuclear Material Management, Orlando, FL, July 19-22, 2004.

9. For more information, see the program section on the U.S. Department of Energy Website at <http://www.nnsa.doe.gov/na-20/program.shtml>.

10. One of the first experts to emphasize the importance of the human factor was Dr. William Potter, director of the Center for Nonproliferation Studies at the Monterey Institute of International Studies. In 1997 Potter defined a "safeguard culture" as a "pervasive, shared belief among political leaders, inspectors, and facilities technicians that MPC&A systems are important and must be carefully operated and maintained." In James E. Goodby, Ronald F. Lehman II, and William C. Potter, *A Comparative Analysis of Approaches to the Protection of Fissile Materials*, CISAC Conference/Workshop Report (Stanford, CA: Center for International Security and Cooperation, 1997). See also James E. Doyle and Stephen V. Mladineo, "Assessing the Development of a Modern Safeguards Culture in the NIS," *The Nonproliferation Review* 2 (winter 1998): p. 91, and Fred Wehling and William C. Potter, "Sustainability: A Vital Component of Nuclear Material Security in Russia," *The Nonproliferation Review* 1 (spring 2000): pp. 180-188. Nathan Busch briefly discusses the issue in his recent book *No End in Sight: The Continuing Menace of Nuclear Proliferation* (Lexington, KY: University Press of Kentucky, July 2004).

is a case of major import. The nation's nuclear material could fall into dangerous hands, with repercussions that can scarcely be imagined. (The report covers all nuclear facilities except those under the exclusive jurisdiction of the Ministry of Defense.) Second, the research team is intimately familiar with the subject matter. For the past several years, the Center for International Trade and Security has collaborated with Russia's nuclear sector in the areas of MPC&A, export controls, and related training. Third, Russia can provide lessons of general use. Mindful of the nation's distinctive traditions and history, we set out to identify the challenges and tasks ahead in this enterprise. The process of developing a healthier security culture there will provide invaluable lessons-learned for other countries embarking on a similar course.

To encapsulate our findings and transmit them to the people who need them most–top and mid-level managers at Russian nuclear facilities and, perhaps, Western donors that may provide the initial impetus to get started–we have attached to this report a tentative training curriculum to help managers begin the arduous task of nurturing security culture within their organizations. Also attached is a generic evaluation methodology to enable them measure their progress toward a healthy security culture. Another appendix includes two case studies describing successful insider diversion operations at a nuclear facility and a gold refining plant. These cases demonstrate how a group of employees intent on criminal action can beat highly sophisticated security measures.

This report is a follow-up to the preliminary study *The Human Factor and Security Culture: Challenges to Safeguarding Fissile Materials in Russia*, which was released by the University of Georgia Center for International Trade and Security in November 2002. ■

C H A P T E R I

SECURITY CULTURE: CONCEPT AND MODEL

1.1 Background

Over the past several years, the International Atomic Energy Agency (IAEA) has aggressively promoted the concept of "nuclear security culture" as a tool to improve the physical protection of nuclear material. Indeed, a 2001 IAEA report titled *Fundamental Principles of Physical Protection of Nuclear Material and Nuclear Facilities* identified security culture as one of the twelve principles underlying fissile-material security (Principle F), emphasizing that:

> All organizations involved in implementing physical protection should give due priority to the security culture, to its development and maintenance necessary to ensure its effective implementation in the entire organization.[1]

A major premise of this report is that basic standards of security culture (defined in some detail below) should be understood the same way from country to country, regardless of differing socioeconomic and political conditions. A uniform understanding of clearly defined standards is important for international exchanges, evaluation, and comparison. In our age of international terrorism and porous borders, moreover, common standards will help discourage those who want to lay hands on fissile materials from seeking easier targets. Even so, each country's approach to achieving those standards will vary according to its history, traditions, and overall professional culture.

The growing threat of catastrophic terrorism and other new security challenges made it obvious that the scope of nuclear security and the associated culture needed to extend beyond the traditional task of protecting weapons-usable material to cover, among other things, radioactive sources and spent nuclear fuel. The message of UN Secretary General Kofi Annan to the 58th General Assembly spoke of deep worldwide concern over the risk of terrorists' acquiring and using nuclear devices or radioactive materials. Annan portrayed the effort to keep nuclear weapons out of such dangerous hands as "a sine qua non of global security." He urged all governments to work closely with the IAEA to take stronger measures to ensure the physical protection, safety, and security of nuclear and radioactive materials.[2]

Not only governments but additional organizations need to be involved in nuclear security. This new strategy must encompass a wide variety of installations and activities. It must account not only for power and research reactors and the related fuel-cycle facilities but also for waste storage sites; research, academic, agricultural, industrial, and medical institutions that work with nuclear and radioactive materials; the vehicles used to transport fissile materials domestically and internationally; and an array of applications involving these materials. Public awareness is likewise indispensable. In the post-September 11 world, consequently, promoting nuclear security culture

1. International Atomic Energy Agency, *Physical Protection Objectives and Fundamental Principles*, GOV/2001/41, Attachment to GC(45)/INF/14, *Measures to Improve the Security of Nuclear Materials and Other Radioactive Materials*, <http://www.iaea.org/About/Policy/GC/GC45/Documents/gc45inf-14.pdf>.

2. UN General Assembly, Press Release SG/SM/9486, IAEA1361UN, September 20, 2004, <http://www.un.org>.

requires not only dedicated leadership within organizations entrusted with fissile materials, but also broad participation at all levels of government, business, and civil society. All participants need to assign high priority to security planning and management. Educating these participants is the best way to assure that nuclear security receives attention and resources commensurate with its importance.

In an effort to reflect these new realities and concerns, a more recent IAEA document, the 2004 *Code of Conduct on the Safety and Security of Radioactive Sources*, urged every state to take appropriate measures to promote safety culture[3] and security culture with respect to radioactive sources. The *Code of Conduct* depicted this cultural approach as a way to protect individuals, society, and the environment.[4] Among other things, the document defined nuclear security culture as "characteristics and attitudes in organizations and of individuals which establish that [nuclear] security issues receive the attention warranted by their significance." At present, however, the IAEA is still working on detailed guidance and recommendations regarding the concept of nuclear security culture, its content, and ways to make it a reality.

1.2 Safety and Security Overlap

Events in the Soviet Union, and later Russia, prodded the world community to begin thinking about safety culture and, subsequently, security culture. The 1986 Chernobyl accident, which resulted primarily from human error and violations of safety regulations, prompted the IAEA to embark on an laborious and time-consuming search for universally acceptable standards of safety culture. By the 1990s it had become obvious that inadequate skills and low motivation in the workforces at Russian sites imperiled international security. The need to develop a security culture, as distinct from a safety culture, is now widely acknowledged. Security culture and safety culture have much in common, but at times their requirements are at odds with one another. IAEA document INFCIRC/225/Rev.4, *The Physical Protection of Nuclear Material and Nuclear Facilities*, captures this ambiguous relationship. Section 7.1.5 of the document declares:

> Safety specialists, in close cooperation with physical protection specialists, should evaluate the consequences of malevolent acts, considered in the context of the State's design basis threat, to identify nuclear material, or the minimum complement of equipment, systems or devices to be protected against sabotage....Potential conflicting requirements, resulting from safety and physical protection considerations, should be carefully analyzed to ensure that they do not jeopardize nuclear safety, including during emergency conditions.[5]

The tension between the two concepts arises from the fact that they embody two fundamentally different approaches to enhancing the operational reliability of vital systems, equipment, and components. Proponents of the engineering approach to safety typically call for building increased redundancy into at-risk systems, while proponents of security culture point out that greater redundancy would render these systems, equipment, and components even more vulnerable to malicious acts–making security even more costly and elusive than it already is. To help identify

3. For more on safety culture, see Ian Barraclough and Annick Carnino, "Safety Culture: Keys for Sustaining Progress," *IAEA Bulletin* 40 (June 1998): pp. 27-30, <http://www.iaea.org/Publications/Magazines/Bulletin/ Bull402/safetyculture.pdf>.

4. International Atomic Energy Agency, *Code of Conduct on the Safety and Security of Radioactive Sources*, 2004, <http://www-pub.iaea.org/MTCD/publications/PDF/Code-2004.pdf>.

5. International Atomic Energy Agency, *The Physical Protection of Nuclear Material and Nuclear Facilities*, INFCIRC/225/Rev.4, June 1999, <http://www.iaea.org/Publications/Documents/Infcircs/1999/infcirc225r4c/rev4_content.html>.

vulnerabilities in safety systems that are relevant to protection against sabotage, the IAEA developed "Guidelines for Self-Assessment of Safety and Security Vulnerabilities of Nuclear Installations."[6] These guidelines identify important synergies between safety and security.

Despite occasional conflict between the tenets of security culture and safety culture, the former is emerging as a distinct and important approach to enhancing physical protection. There are several reasons to develop a distinct concept of nuclear security culture:

- The concept of safety culture has been widely applied within the nuclear power industry, but it is not generally familiar to the wider range of organizations involved with nuclear materials and radioactive sources.
- Some aspects of security (e.g., controls over access to classified information, or the fact that the threat is purposeful rather than accidental or caused by equipment failure) differ from the safety field.
- While the objectives or desired outcomes of a nuclear security regime overlap to a substantial degree with those of a nuclear safety regime, they are not identical: It is possible to be safe without being secure.

Notwithstanding the tension between the two concepts, the characteristics of a good security culture would likely result in improved safety, quality, and productivity in an organization, since closer attention to personnel performance tends to produce better results in every area. Conversely, an improved safety culture would ideally make breaches of security less likely. The 2003 IAEA General Conference acknowledged such linkages and noted, among other things, that strengthening the safety of radioactive sources helps enhance the security of these sources.[7]

1.3 Nuclear Security

The IAEA Advisory Group on Nuclear Security, established in January 2002, defined nuclear security as:

> The prevention and detection of, and response to theft, sabotage, unauthorized access, illegal transfer or other malicious acts involving nuclear material, other radioactive substances or their associated facilities.[8]

This broad interpretation is largely consistent with the guidelines set forth in UN Security Council resolution 1540 of April 28, 2004, which sought to prevent the spread of weapons of mass destruction (WMD). The resolution is innovative in that, for the first time in such a document, it elaborates a comprehensive vision of how to curb the supply side of the proliferation problem. Among other

---

6. Tomihiro Taniguchi and Anita Nilsson, "Hot Spots, Weak Links: Strengthening Nuclear Security in a Changing World," *IAEA Bulletin* 46 (June 2004), <http://www.iaea.org/Publications/Magazines/Bulletin/Bull461/hot_spots.html>.

7. International Atomic Energy Agency, "IAEA General Conference Resolution," GC(47)/RES/8, September 2003, <http://www.iaea.org/NewsCenter/Statements/2004/ebsp2004n008.html>.

8. The IAEA's working definition of nuclear security, as adopted by the IAEA Advisory Group on Nuclear Security, is quoted in Taniguchi and Nilsson, "Hot Spots, Weak Links": p. 60. The Convention on the Physical Protection of Nuclear Material and Nuclear Facilities defines sabotage as "any deliberate act directed against a nuclear facility or nuclear material in use, storage or transport which could directly or indirectly endanger the health and safety of personnel, the public and the environment by exposure to radiation or release of radioactive substances." International Atomic Energy Agency, "Convention on Physical Protection of Nuclear Material," INFCIRC /274/Rev.1/Add.7, September 22, 2000, <http://www.iaea.org/Publications/Documents/Infcircs/2000/infcirc274r1a7.pdf>.

things, the main body of the resolution requires all states to:

- develop and maintain appropriate effective measures to account for and secure WMD-related items in production, use, storage, or transport
- develop and maintain appropriate and effective physical protection measures to safeguard these items

Just as striking is the fact that Security Council resolutions issued under Chapter VII of the UN Charter, as resolution 1540 was, are binding on all UN member states. UN member states thus are now accountable for implementing the terms of the resolution, regardless of whether they are parties to the relevant treaties, agreements, and regimes.

This report focuses on specific threats such as theft, sabotage, unauthorized access, illegal transfer, and malicious acts that are largely dealt with through material protection, control, and accounting (MPC&A). Accordingly, this section provides an overview of nuclear security in fairly non-technical terms so that the discussions of the cultural aspects of security analyzed below can be kept in context.

Nuclear security starts with understanding what represents a potential target for an adversary, attempting to define how the adversary might threaten this target, and producing appropriate measures to meet the threat. The IAEA recommends the "Design Basis Threat" (DBT) methodology as a tool to design appropriate security measures. In essence, DBT describes the capabilities, intentions, attributes, and characteristics of potential adversaries who might attempt malicious acts. A physical protection system (PPS) for nuclear materials is designed against this threat profile, allowing management at a facility to identify all targets under their control and know what they are protecting. Using the DBT methodology also allows management to rank the vulnerability of targets. In essence, then, the nuclear security regime is founded on a "graded" approach that mounts an in-depth defense of facilities and materials against the greatest and most likely threats.

The first two objectives of a protection system are to deter people from attempting to gain unauthorized access to nuclear facilities and material, and to prevent them from doing so if deterrence fails. Deterrent measures include installing highly visible, imposing security arrangements which convince potential adversaries that they cannot defeat the physical protection system. The problem with deterrence is that its effects are difficult to measure and predict. Related to deterrence is prevention, whose objective is to ensure that potential adversaries are identified and apprehended before they can attempt to gain unauthorized access. Sometimes the intelligence agencies or police forces learn in advance that some person or group is about to attempt a malicious act against nuclear facilities or material. Often, however, tips come from members of the general public. Prevention and detection can therefore be strengthened by a carefully organized public outreach program.

If deterrence and prevention fail, the protection system must detect the attempt to breach security and respond without undue delay–stopping the malicious act before it can be completed. These objectives are accomplished by the physical protection system and the material control and accounting (MC&A) system, which ideally operate in close coordination, constituting the material protection, control, and accounting system for any given facility.

Several elements comprise a PPS. First, detection involves sensing an intrusion, sounding the alarm and assessing the reasons for the alarm, and restricting entry to prospective targets. Second, delay elements, usually passive and active barriers, make the task of breaching security consume more time than it takes to deploy the third element, the security response force, to neutralize the adversary. The three elements must work together harmoniously to achieve optimal results. The effectiveness of any physical protection system, however, depends on how well it is operated and

maintained. A sound overall design can be rendered ineffective by a lack of spare parts, shortfalls in funding for preventive maintenance and repairs, or low morale or negligence among the operating personnel or protective force. High standards of nuclear security culture are partly intended to remedy these deficiencies.

PPS designers analyze the performance of the detection, delay, and response elements in relation to the DBT and the consequences associated with the loss of or damage to the materials being protected. This analysis yields the consequence-weighted risk (Risk = Probability x Consequence), which is the primary metric for gauging whether a physical protection system is adequate. Risk calculations also estimate how well the PPS is likely to perform if one or more of its elements is degraded.

MC&A systems maintain an inventory of the nuclear materials entrusted to a facility, including the specific locations of the materials. These systems also impose stringent controls on the movement and transfer of these materials. The extent and rigor of these systems vary by the type of material and the potential consequences of its unauthorized use. MC&A systems are therefore designed to ensure, on a near-real-time basis, that no material has been illegally transferred from its designated storage site. High standards of MC&A in an organization can deter an employee who might be contemplating theft. If the item accounting system or the bulk-material accounting system indicates that material is missing, this constitutes detection. Detection triggers a response. The response may be to immediately stop all movement of personnel into and out of the facility until the lost material is retrieved, or to start the preplanned hazard mitigation process jointly with other players.

As is the case with the PPS, the ultimate effectiveness of any MPC&A system depends not only on the design and condition of installed equipment and the comprehensiveness of relevant procedures and instructions, but also on the attitudes and behavior of the personnel assigned to use the hardware. As any engineer will attest, equipment and procedures are no better than the operator. Ultimately this "human factor" determines whether a nuclear security regime succeeds or fails. Cultivating a nuclear security culture, then, is as crucial to success as are spare parts and written directives. This range of security requirements determines the nature of nuclear security culture, which can be characterized by:

- ***the degree to which all personnel, from senior managers and supervisors down to the most junior operators, are aware of and committed to widely understood security requirements and best practices***
- ***the degree to which available and affordable security technology is put to use, kept in good working condition, and improved***
- ***the degree to which security regulations and procedures are implemented and personnel are motivated to accomplish their security-related tasks***

1.4 Model of Nuclear Security Culture

A cultural approach to physical protection involves determining what attitudes and beliefs need to be established in an organization, how these attitudes and beliefs manifest themselves in the behavior of assigned personnel, and how desirable attitudes and beliefs can be transcribed into formal working methods to produce good outcomes, i.e., effective protection. An important function of security culture is that it places great weight on the instinctive behavior of personnel. An efficacious security culture expects employees to take a proactive, security-value-based stance in any situation in which nuclear material and/or the facility itself are at risk. It expects them to innovate, since risks are too numerous to predict and no amount of planning or policymaking can prepare them for all contingencies. At a facility that boasts a supportive security culture, then, employees will respond to security issues out of carefully nurtured and proactive habit rather than improvised effort. In an unsupportive security culture, employees and management tend to ignore security, or even to circumvent security precautions when they become inconvenient or costly.

Cultures are based on a set of shared, underlying assumptions about reality (see Figure 1). In the practical context, this means that an organization will display tangible behaviors that derive from what the organization assumes should be most important to it. Often, however, these assumptions are unconsciously held and never discussed in the daily course of business. They simply become "the way we do things," as opposed to a culture that demands conscious attention if it is to survive and thrive.[9] Staff members will form their own assumptions based on their own experiences, or even their whims. The assumptions underlying the organizational culture will atrophy, consequently, unless the leadership works actively to propagate them. Forging and maintaining healthy patterns of ideas is one of the foremost missions of top managers.

A good security culture has to be founded above all upon a healthy respect for the threat (see Figure 1, A-1). From the most senior leadership down to the lowliest technician, the staff has to believe that there is a credible threat to the facility and thus that security measures truly matter. This underlying conviction then permeates the way people do their work, and it drives their behavior under normal and abnormal conditions. In a facility that enjoyed a good security culture, personnel would display a deep-rooted belief that there were credible insider and outsider threats, including theft, sabotage, unauthorized access, illegal transfer, and other malicious acts, and that it was their duty to counteract these threats.

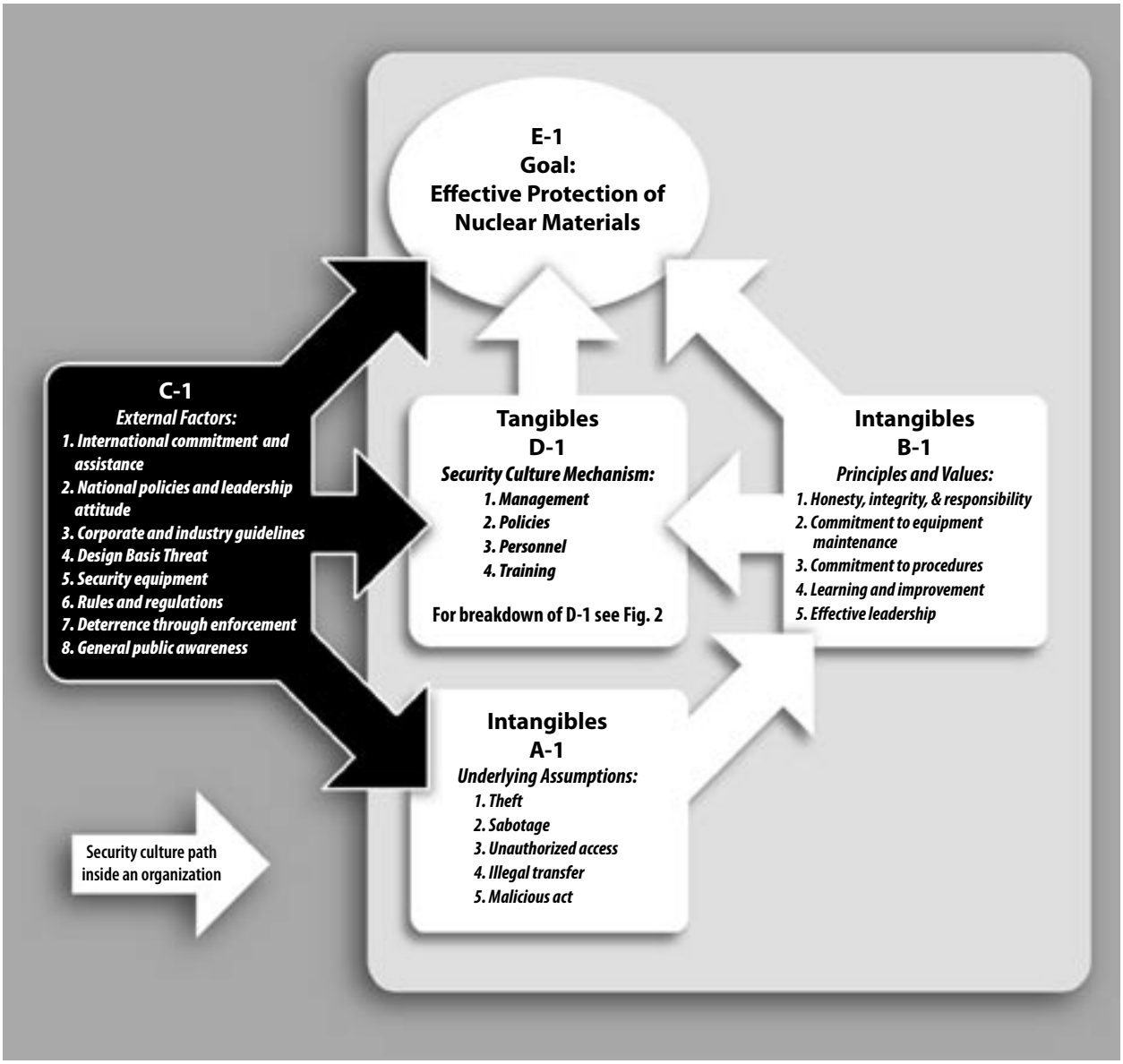
The next level up in deconstructing the underlying assumptions is to conceptualize principles and values conducive to the behaviors and physical arrangements that make up a vibrant security culture (see Figure 1, B-1). These intangible principles and values include honesty, integrity, and a sense of responsibility; a commitment to keeping installed equipment in good working order; compliance with procedure; a commitment to learning and process improvement; and effective leadership throughout the organizational hierarchy. It bears mentioning that these traits are not confined to security. They are a mainstay of healthy management practices. Conversely, a poorly managed work environment that lacks these attributes will be indifferent to efforts to achieve a high standard of security culture. Any campaign to promote nuclear security culture–whether nationally sponsored or funded primarily through international assistance–must seek to better the overall professional culture.[10]

Another major source that shapes the tangible behaviors and concrete attributes identified in Figure 1 as the "Security Culture Mechanism" is a set of eight external factors (see Figure 1, C-1).

---

9. For more on the role of leadership, see James MacGregor Burns, *Leadership* (New York: Harper & Row, 1978); John P. Kotter, *Leading Change* (Cambridge, MA: Harvard Business School Press, 1996); Carnes Lord, *The Modern Prince: What Leaders Need to Know Now* (New Haven, CT: Yale University Press, 2003).

Figure 1. Model of Nuclear Security Culture



10. For more information on organizational and professional culture, see for instance J. Steven Ott, *The Organizational Culture Perspective* (Pacific Grove, CA: Dorsey Press, 1989); Edgar H. Schein, *Organizational Culture and Leadership*, 3d ed. (San Francisco, CA: Jossey-Bass, 2004); Hal Rainey, *Understanding and Managing Public Organizations* (San Francisco: Jossey-Bass, 2000); John P. Kotter and J. L. Heskett, *Corporate Culture and Performance* (New York: Macmillan, 1992); Alan L. Wilkins, *Developing Corporate Character: How to Successfully Change an Organization Without Destroying It* (San Francisco, CA: Jossey-Bass, 1989); U.S. Office of Personnel Management, *A Handbook for Measuring Employee Performance* (Washington, DC: Government Publishing Office, 2001). Another area of organizational theory related to the problems discussed in the report is known as *diffusion of innovation*. Everett Rogers (*Diffusion of Innovations*, 5th ed. (New York: Free Press, 2003)) defines diffusion as the process by which, over time, an innovation is communicated through certain channels among the members of a social system. Rogers's definition contains four elements that are present in the diffusion-of-innovation process. The four main elements are: (1) innovation–an idea, practices, or objects that are perceived as new by an individual or other unit of adoption; (2) communication channels–the means by which messages get from one individual to another; (3) time, including three time factors–(a) innovation-decision process, (b) relative time within which an innovation is adopted by an individual or group, and (c) the rate of adoption of an innovation; (4) social system–a set of interrelated units that are engaged in joint problem solving to accomplish a common goal.

These are independent variables that can either hamper or facilitate the development of security culture in an organization. External factors include:

1. *International commitments and assistance.* Membership in relevant international agreements and forums facilitates the promotion of nuclear security culture. Since September 2001, working in Europe, Asia, Latin America, and Africa, the IAEA has conducted over 50 security advisory and evaluation missions and convened over 60 training courses, workshops, and seminars.[11] IAEA programs relevant to security culture include the International Physical Protection Advisory Service (IPPAS), which upon request helps member states evaluate their physical protection systems at the state and facility levels. The work of the IPPAS is based on the recommendations contained in document INFCIRC/225[12] and the obligations set forth in the Convention on Physical Protection of Nuclear Material.[13] The IAEA is also developing Integrated Nuclear Security Support Plans with individual member states, as frameworks for helping to address their nuclear security needs over the longer term. External MPC&A assistance from sources such as the U.S. Department of Energy's program in Russia and the other former Soviet republics contributes significantly to the familiarization process and the actual MPC&A infrastructure.

2. *National policies and leadership attitude.* The behavior of management and other personnel at a facility reflects the priority accorded nuclear security issues by the national leadership. When top political leaders demonstrate their interest in this vital area, they send a powerful signal down to staff members at individual sites.

3. *Corporate and industry guidelines.* A clear division between regulatory and operating functions is a must for sustaining industry-wide security standards. Industry and the appropriate agencies are responsible for clarifying and updating the current threat assessment in addition to conducting training, inspections, and quality assurance. Funding issues ranging from budgetary allocations to recommendations for private operators also fall under the purview of industry.

4. *Design Basis Threat.* As mentioned previously, the IAEA recommends DBT as the best method to design security measures, since it takes into account the capabilities, intentions, attributes, and characteristics of potential adversaries. Drawing on this methodology, individual countries can develop their own DBTs consistent with best practices and national traditions and history.

5. *Security equipment.* This equipment must be available through appropriate channels, meet national and international standards, and stay affordable by coming in a variety of price ranges–allowing sites with smaller budgets to sustain their security precautions. The ultimate goal is to make optimal use of automated processes and procedures, thereby limiting prospects for human error.

6. *Rules and regulations.* The texts of written directives, in addition to the overall legal basis, must be up-to-date, succinct, and user-friendly. This is especially true for personnel who do not routinely deal with security matters. These texts need to send a clear and unambiguous message.

7. *Deterrence through enforcement.* National governments should criminalize activities that might lead to breaches of nuclear security. The appropriate government agencies need to enforce these laws rigidly in order to deter potential perpetrators.

---

11. Mohamed ElBaradei, "Nuclear Proliferation and the Potential Threat of Nuclear Terrorism," Presentation at Asia-Pacific Nuclear Safeguards and Security Conference, Sydney, Australia, November 8, 2004, <http://www.iaea.org/NewsCenter/Statements/2004/ebsp2004n013.html>.

12. International Atomic Energy Agency, *The Physical Protection of Nuclear Material and Nuclear Facilities*.

13. International Atomic Energy Agency, "Convention on Physical Protection of Nuclear Material and Nuclear Facilities."

8. *General public awareness.* The escalation of terrorism in recent years has created a political climate in which the public is receptive to security concerns. Well-tailored outreach efforts, consequently, can convince the public that breaches of security could jeopardize the safety of nuclear facilities, and even their own lives. A public that starts caring about security will be more likely to (a) report attempts at diversion and terrorism; (b) report inadequate security perimeters, suspicious people near a facility, and other conditions that could contribute to a breach of security; (c) call media, government, and legislative attention to security problems at nuclear facilities; and (d) form advocacy groups to publicize the importance of nuclear security.

The ultimate goal of the "Model of Nuclear Security Culture" (Figure 1) is to contribute to the efficient protection of nuclear material. This goal can be achieved by managing, among other contributing factors, the three distinct but interacting sets of inputs discussed above: Principles and Values (B-1), External Factors (C-1), and the Security Culture Mechanism (D-1). These inputs are unique and equally important. Since it represents the primary focus of this report, however, the Security Culture Mechanism receives the bulk of the attention in the next section.

1.5 Model of Security Culture Mechanism

The purpose of this section is to outline the tangible structures and behaviors within an organization (designated D-1 in Figure 1), which we call the Security Culture Mechanism. This mechanism, described more fully in Figure 2,[14] is broken down into four major units: Facility Leadership (A-2), Proactive Policies and Procedures (B-2), Personnel Performance (C-2), and Learning and Professional Improvement (D-2). Each major unit is further broken down to permit brief comments and clarifications, which are offered on a selective basis.

In order to understand the workings of this mechanism, it is useful to look again at some general properties of nuclear security culture:

- Cultures are a product of social learning. Therefore, they cannot be shifted without determined effort from national and facility leaders. Orientation sessions that provide an outlet for explanation and discussion can help leaders modify the organizational culture, provided they back up these sessions with daily reinforcement and leadership-by-example.
- Cultures are difficult to enforce, but they can be developed, primarily through positive reinforcement and role models.
- There is always a security (or safety, or quality, etc.) culture in an organization. The questions are whether the culture is what management needs it to be, and whether it is improving, decaying, or remaining static.
- It is often easier to change patterns of thinking in an organization than to change patterns of behavior. New managers can come in brimming with bold new ideas, for example, yet fail to get people to change their old behaviors.
- Leaders change the organizational culture by intervening at all levels. With sustained effort, and by deploying the incentives and disincentives at their disposal, they can mold new patterns of thinking, establish new patterns of behavior, and even change the physical environment.

14. The authors recognize the need to rank-order these subcategories according to priority, but this task is specific to each country and must be accomplished by surveying a pool of national experts in the field.

- Cultures reduce anxiety for their members by establishing shared patterns of thinking, speaking, and acting. Consequently, cultural change will always increase anxiety within the organization until the new patterns are learned. Leaders must make the anxiety of learning a new culture less than the anxiety of staying in the old culture.

Nuclear facilities to which the Security Culture Mechanism applies include nuclear power plants, fuel-cycle facilities, research reactors, and defense facilities which handle or store nuclear material. These facilities are normally subject to nuclear security regulations, and they have departments or functions that are responsible for security. Several security problems typify such facilities. A strong sense of vulnerability to the insider threat, for instance, may be missing. People have often served at these organizations for long periods of time, and they cannot bring themselves to believe that their long-time colleagues and friends would steal nuclear materials.

This problem is especially pronounced at facilities located in remote areas, where the work community overlaps substantially with the social community. Another problem arises from the financial pressures on these facilities, which in turn are the cause of resource shortages and operational problems. Nuclear security tends to rank low on the scale of priorities when the survival of the organization is at stake. An overall lack of commitment to nuclear security can result. Finally, as with any organization, individuals may fail to demonstrate personal responsibility, and management may tolerate low standards of honesty and integrity.

The Security Culture Mechanism framed in Figure 2 is designed to operate inside the abovementioned facilities, contributing to a security-conscious work environment. Its main element is the performance of leadership. Top managers are responsible for developing and implementing a specific set of policies and procedures that shape the behavior of their subordinates. Continuous training is one of the available tools to get the required results. Below are comments and clarifications regarding the policies detailed in Figure 2:

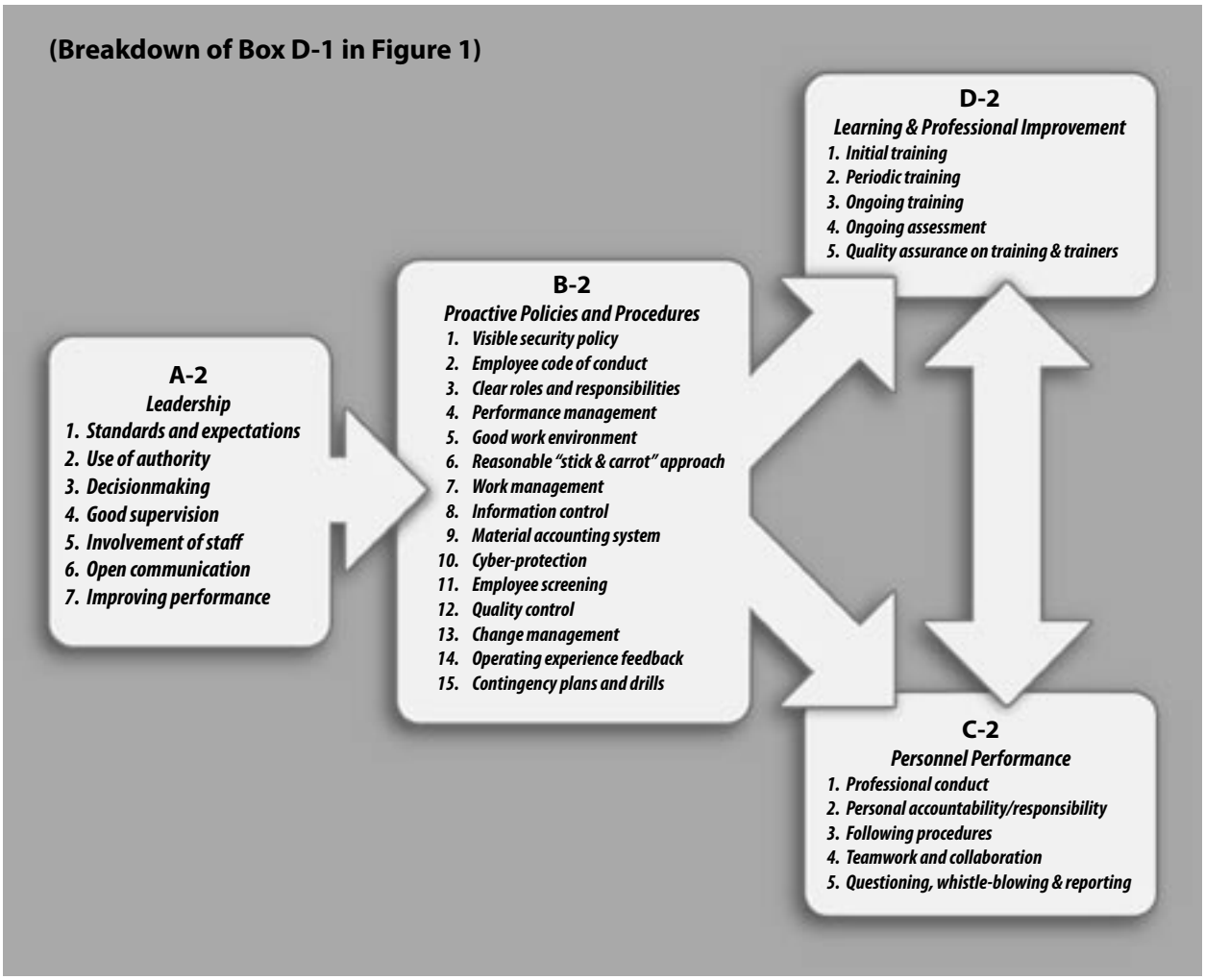
Leadership:

- A-2/4. *Good supervision*. An effective nuclear security culture depends upon the behaviors of individuals. Behavior in turn is very strongly influenced by good supervisory skills–skills that should be honed through training programs.
- A-2/5. *Involvement of staff*. The performance of an organization improves when all levels of the staff are empowered to contribute insights and help solve practical problems. Mechanisms should be in place to encourage the staff to take ownership of the facility's work.
- A-2/6. *Open communications*. Consistent with information security, encouraging and maintaining a free flow of information up, down, and horizontally within an organization is intrinsic to a good security culture.
- A-2/7. *Improving performance*. An organization that is not constantly trying to improve its performance will become complacent. Complacency is a precursor to a serious decline in security standards and even breaches of security.

Proactive Policies/Procedures:

- B-2/1. *Visible security policy*. A policy document should exist which states the commitment of the organization to nuclear security, and which establishes the highest level of expectations with respect to decisionmaking and conduct. This mission statement should be promulgated widely throughout the facility.

Figure 2. Model of Security Culture Mechanism: Management, Policies, Personnel & Training



- B-2/2. *Staff code of conduct.* It is especially important in the field of security to assure that staff members know what is expected of them. They will be expected, for example, to protect sensitive information, remain vigilant about potential security concerns, threats, and unusual occurrences, and bring security-related matters to the attention of their supervisors.
- B-2/3. *Clear roles and responsibilities.* All organizations need to delineate clearly "who is responsible for what" if they are to achieve their desired results. The organizational structure must be revised and updated, preferably beforehand, when organizational change is planned.
- B-2/7. *Work management.* Nuclear security equipment will require periodic maintenance, repairs, and modification. All work on equipment should be planned to ensure that security coverage is adequate while the equipment is off-line.
- B-2/9. *Material accounting system.* The accounting systems for nuclear materials and radioactive substances are a vital part of the nuclear security system and must be vigorously supported and operated by qualified personnel.
- B-2/10. *Cyber-protection.* Security-related electronic information needs to be shielded from unauthorized access and use. A cyber-protection system featuring, for instance, firewalls and virus protection should be in place and should be routinely audited for effectiveness.

- B-2/11. *Staff screening*. Any security barrier or procedure can be defeated, particularly with insider collaboration. Effective staff screening processes and established procedures are essential. The facility's own security staff or, if necessary, external law-enforcement agencies can carry out personnel screening to diminish the likelihood of an inside job.
- B-2/13. *Change management*. Many if not most organizational problems and failures are traceable to inadequate management of change. This applies not only to changes in equipment and procedures, but also to changes in organizational structures and roles, turnover in the workforce, and so forth. Therefore, the organization needs to institute processes to understand, plan, implement, and reinforce change–especially change relating to the security function.
- B-2/15. *Contingency plans and drills*. Most of the overall nuclear security system is poised to respond to an event, but it is rarely triggered by an actual event. Accordingly, management needs to conduct frequent drills to test out the organization's capacity to respond to attempted or successful malicious acts or significant breaches of its defenses.

Personnel Performance:

- C-2/2. *Personal accountability*. Accountability means that all personnel know their specific assigned tasks–what they have to accomplish, by when, and what good results look like–and that they either execute these tasks or report to their supervisors if they are unable to execute them. If management fails to hold workers responsible for the performance of their duties, the performance of the organization as a whole will suffer.
- C-2/3. *Following procedures*. Procedures embody the organization's collective knowledge and experience, and they must be followed to ensure that tasks are performed correctly. To help the staff comply with established procedures, managers must assure that procedures are clear, up-to-date, and easy to find and use.
- C-2/5. *Questioning and reporting*. Because security depends on vigilance and on "expecting the unexpected," management must encourage the staff to be observant and to question small discrepancies as a matter of routine. This habit may prove difficult to instill in nations where authoritarian governments once discouraged employees from questioning authority and encouraged them to inform on their peers.

Learning and Professional Improvement:

- D-2/1. *Initial training*. New employees should receive baseline instruction on policies, issues, and incident response/reporting procedures. The training should be tailored to an individual's job within the facility, and it should be short enough to be easily comprehensible. Accession training can range from classroom instruction to computer-driven self-study modules. New employees should be quizzed briefly to assure that they grasp the essential elements of the training, and they should be required to sign a statement certifying that they understand its content.
- D-2/2. *Periodic training*. The essential elements from the initial training should be reviewed regularly. Special sessions should be held when policies and procedures are updated. Attendees should be quizzed again to assure comprehension and required to sign a new statement verifying their attendance. Refresher training can be performed annually, quarterly, or as needed.
- D-2/3. *Ongoing programs*. Ongoing programs are one of the most effective tools available to the security-conscious facility. They include traditional methods such as wall posters, handouts, and memos, as well as more interactive methods such as monthly email updates and special bulletins reviewing the lessons-learned from internal and external security incidents.

- D-2/4. *Ongoing assessment.* This will vary considerably, depending on the resources available to the facility and the facility's actual security needs. Still, management should conduct appropriate and random assessments to ensure the training is effective. Top managers should drop in on training sessions unannounced.
- D-2/5. *Quality assurance on training and trainers.* It is important to elicit feedback on the training programs and materials, as well as the trainers themselves. Those responsible for training should include quality assessment as part of the program. Feedback should be requested of those who undergo the training, in the form of post-training evaluations. The insights gleaned from the evaluation process should be used to refine the training curriculum.

The performance of a nuclear security regime ultimately hinges on how people behave. A workforce made up of individuals who are vigilant, question irregularities, execute their work diligently, and exhibit high standards of personal and collective behavior will maintain tight security. Management must do its part. Managers must apprise workers of what is expected of them, encourage them to do the right thing, and dole out rewards and punishments to shape their behavior. Failures of leadership are the most common single problem besetting an organization that needs to improve its nuclear security culture.

Having reviewed the tenets of nuclear security culture, this report will now focus in on Russia as a case study. The following chapters examine the security regimes at Russian nuclear facilities and discuss the current status of security culture in Russia. Among the questions to be answered are: To what extent are Russia's political and industrial leaders committed to better nuclear security? Do these leaders have the organizational acumen and the funding to generate higher security standards at the facility level? Do Russia's perception of the threat and security requirements differ from those of the West, and, if so, with what consequences? What can be done to reshape the mentality of the personnel entrusted with security, and to introduce effective security culture standards? Answering these questions will help policymakers in Russia–and beyond–bolster international security. ■

C H A P T E R II

HARDSHIPS OF ECONOMIC AND POLITICAL TRANSITION

The political and economic collapse of the Soviet Union had a wide-ranging, deleterious effect on the country's nuclear industry and on the security of its nuclear materials. The reforms undertaken by the Russian government during the 1990s created conditions that left the nuclear industry at once underfunded and understaffed. Despite shrunken budgets, the industry was compelled to compete for workers who were struggling to make ends meet, who were losing their patience and loyalty to their employers, whose technical proficiency was atrophying in the meantime, and who were lured from the industry by higher-paying jobs elsewhere. Among the conditions directly or indirectly undermining security were:

- a weak economy that could barely support the basic needs of the nuclear sector, let alone costly efforts to upgrade security arrangements
- the deteriorating physical condition of the country's infrastructure, hardware, and communications
- a federal system in decline
- rampant corruption that ensnared many officials, from junior bureaucrats to senior government policymakers
- a surge in organized crime that took control of some aspects of the remnants of the economy
- soaring rates of alcohol consumption and drug abuse among the population

In short, the nuclear sector was exposed to the developments that convulsed Russian society, but it was more cautious than many sectors about embracing the ideological and organizational reforms that soon swept the country. Its continuing reliance on old approaches to nuclear-material security amid these new realities hampered efforts to enhance security standards and implant a new mentality that was more hospitable to security.

2.1 Weak Economy and Insufficient Funding

The Soviet nuclear industry depended almost exclusively on government funding and consequently had little experience with marketing and selling its products, either on the domestic market or abroad. As a result of the sharp decline in Russia's gross domestic product and the federal budget, the defense sector, including its nuclear component, lost almost 80 percent of its funding during the 1990s.[1] The Ministry of Atomic Energy (Minatom) was hit hard during the 1998 financial crisis, when the federal government funded only 20 percent of its operating expenses.[2] Even the cash-generating nuclear power plants were in dire straits, with some unable to pay their taxes and some

1. "Military Industry Overview," Federation of American Scientists Website, <http://www.fas.org/nuke/guide/russia/industry/overview.htm>.

2. Igor Khripunov, "Minatom at the Edge," *Bulletin of the Atomic Scientists* 55 (May/June 1999), <http://www.thebulletin.org/issues/1999/mj99/mj99khripunov.html>.

facing bankruptcy. Defense nuclear facilities delayed paying salaries and were forced to scramble to commercialize some of their activities. According to former Minatom Minister Victor Mikhailov, the volume of government contracts for defense nuclear items in 1996 had plummeted to 25 percent of the 1988 figure. This drop-off spurred massive unemployment (as reflected both in official and in unofficial figures) and salary shortages.[3]

To make matters even worse, many Russian nuclear facilities had been set up in remote locations to maintain the necessary level of secrecy. Ten such closed nuclear facilities currently remain in Russia.[4] For many workers and engineers employed at a closed facility, the surrounding small town was the only place they had ever lived, the facility was the only employer they had ever had, and the entire social infrastructure was provided by the facility. This setup was reminiscent of the early- and mid-20th-century U.S. factory towns, with similar advantages and pitfalls. The manager of the facility doubled as the unofficial mayor and city manager. He was involved as much in the problem of supplying foodstuffs and consumer goods to the city's stores as in fulfilling the government's production plan. The relationships between workers and management at such facilities were built on trust, loyalty, and the bond of living and surviving together in a remote location, often under hostile environmental conditions. As unemployment rose and budgets plunged, the morale at these remote facilities fell precipitously.[5]

Nuclear-sector employees felt betrayed and resentful when the political and economic reforms undertaken by the government left their industry in shambles. From the late 1940s forward, weapons-grade fissile materials had been produced at a tremendous cost in lives and opportunity. To fulfill their patriotic duty, physicists had traded the comfort of big cities for deprivation and long hours at remote defense installations. These lifelong sacrifices and dedication no longer appeared to be needed or appreciated in post-Soviet Russia. The country was moving rapidly into the privatization stage, and defense facilities were ordered to quickly convert their production lines to manufacture consumer goods. The conversion effort took place without proper forethought, investment, retooling, market research, or retraining efforts. The older generation of nuclear workers, which was closing in on retirement, went without a meaningful social safety net.

The dismal condition of the defense nuclear sector throughout the 1990s caused a public outcry. Wage arrears reached months. Many employees went to work every morning to keep busy, even though they had not been paid. Managers sought to keep their workforces going without proper budget authorization from the government. Nonviolent demonstrations and marches took place with alarming frequency. Suicides were reported among both rank-and-file employees and well-known nuclear scientists and engineers. The pro-Communist opposition media exploited the situation to advance its agenda.[6] Scores of scientists and engineers fled the industry to pursue jobs that could earn them at least a sparse living, but that had nothing to do with their primary skills and training.[7] An entire generation of scientists and engineers was lost: Graduates of the most prestigious universities and institutes in the fundamental and applied sciences chose to pursue

---

3. Victor Mikhailov, "Nuclear Energy Potential and Issues of Conversion," *Konvesriya Oboronnoy Promyshlennosti* 1 (1996), <http://www.iss.niiit.ru/70/art-045.htm>.

4. These are primarily nuclear-weapons research and manufacturing facilities, as well as sites for producing and disposing of highly enriched fissile materials and spent nuclear fuel.

5. For more information, see for instance Sarov Analytical Nonproliferation Center and Institute of Strategic Stability, *Nuclear Tests in the USSR, 1949-1990* (Snezhinsk, Chelyabinsk: VNIITF, 1996), <http://www.npc.sarov.ru/issues/peaceful.html>; Valentin Tikhonov, *Russia's Nuclear and Missile Complex: The Human Factor in Proliferation* (Washington, DC: Carnegie Endowment for International Peace, 2001); Gennady Zhuravlyov, *From Theory to Practice: Psychological Foundations of Safety Culture in Nuclear Energy and Industry* (Moscow, 1998).

6. P. Mesnyankin, "The Collapse of the Nuclear Center," *Zavtra* 42 (October 20, 1998), <http://www.zavtra.ru/cgi/veil/data/zavtra/98/255/42.html>.

7. For the situation in the nuclear sector, see for instance Igor Khripunov and Maria Katsva, "Russia's Nuclear Industry: The Next Generation," *Bulletin of the Atomic Scientists* 51 (March/April 2002): pp. 53-54.

other careers, fearing for their job security if they opted to join the nuclear industry. The brightest young students sought degrees in economics or marketing instead of physics or engineering.[8]

Against this disheartening backdrop, a major contribution to nuclear security came from outsiders. Financial assistance from the United States and other Western donors played, and continues to play, an important role in the effort to improve physical protection at nuclear installations. In recent years, anywhere from 30 to 50 percent of the total funding available for physical protection has come from foreign donations.[9] Issues associated with material protection, control, and accounting (MPC&A) have been addressed through the Nunn-Lugar Cooperative Threat Reduction Program, the Materials Protection, Control, and Accounting Program, the Nuclear Cities Initiative, the G-8 Global Partnership Against the Spread of Weapons and Materials of Mass Destruction, and an assortment of other programs. Total funding for these programs came to an estimated $5 billion over the past decade. A substantial fraction of that was invested in upgrading security arrangements at Russia's nuclear facilities.[10] Seventy percent of the facilities involved have substantially improved and upgraded their security and material accounting systems as a result of this effort. The U.S. Department of Energy's (DOE) rapid upgrades program had helped secure nuclear material at 40 Russian nuclear sites by the end of 2003.[11]

The gradual stabilization of the Russian economy from the late 1990s forward helped address some of the deficiencies in nuclear security. Although some problems persist, the situation is not as dire as it was in the early 1990s: In general, facility employees and security guards are paid on time, salaries have risen, and some of the financial and infrastructure pressures have eased.[12] As Russia's economy continues to grow and its oil/gas export revenues rise, the Russian government will likely supplement foreign assistance projects by boosting funding and crafting policy decisions, documents, and regulations that guide the chain of command, all the way from the government, through the newly created Federal Atomic Energy Agency (FAEA, or Rosatom), down to the level of individual facilities. According to Rosatom Director Alexander Rumyantsev, his agency has been receiving steady federal funding for all critical defense nuclear programs–a fact that should allow Rosatom and the government in general to devote greater resources to improving security at all nuclear installations.[13]

Nevertheless, the shortfalls in resources and attention for the defense and nuclear sectors during the 1990s produced a lasting negative effect on the industry, which continues to manifest itself in poor quality and reliability of even the most sophisticated and competitive Russian products, weapons systems, and hardware. Experts have voiced concern not only with falling quality standards, but also with the apparent indifference of officials and managers to the problem.[14]

---

8. A number of Russian scholars have focused on this generational gap and the need to fill it. Authors' interview with a lab director at Perm University, February 5, 2002.

9. International Business Relations Corporation, "Foreign Trade Policy and Authorized Foreign Trade Entities of the Ministry of RF for Atomic Energy," *IBR Report* (Moscow, 2003).

10. International Department, Rosatom Website, <http://www.minatom.ru/about/department/dmvs/itogi.doc>.

11. Charles T. Bolton, Lorilee Brownell, and William J. Toth, "The Department of Energy's Approach to Sustainability," Paper Presented at the 45th Annual Meeting of the Institute of Nuclear Material Management, Orlando, FL, July 18-23, 2004. Rapid upgrades consist of low-cost items such as locks, material cages, and hardened doors and windows. About 132 tons of this material has received more comprehensive upgrades, including closed-circuit television, sensors, and sophisticated material measuring equipment.

12. For a useful discussion of the effect of Russian economic and political stabilization on nuclear security see Matthew Bunn and Anthony Wier, *Securing the Bomb: An Agenda for Action* (Cambridge, MA: Belfer Center for Science and International Affairs, Harvard University, May 2004), pp. 30-34, <http://bcsia.ksg.harvard.edu/BCSIA_content/documents/securing_the_bomb.pdfwww.nti.org/cnwm>.

13. Andrey Garavskiy, "Russian Defense Ministry Will Oversee the Atom," *Krasnaya Zvezda*, August 11, 2004.

14. See for instance Andrey Babakin, "Defective Equipment Undermines National Security," *Nezavisimoye Voennoe Obozrenie*, August 6, 2004.

To help maintain the safety and security of its nuclear materials, Russia has developed and adopted a special federal program titled "Nuclear and Radiation Safety and Security in Russia for the Years 2000-2006." The program consists of 20 subprograms, several of which have a direct bearing on nuclear security.[15] The adoption of this program represented the first sustained attempt by the Russian government to address the issue of nuclear-material security, among other things. The program targets nuclear safety and security. The former, however, claimed a disproportionate share of attention and resources, both in terms of the number of subprograms and the amount of available funding. The program provided a maximum of only $5 million over the course of six years to improve MPC&A at nuclear facilities and to train the relevant personnel.

According to Yuri Vishnevskiy, a former director of Russia's Federal Nuclear and Radiation Oversight Agency (GAN, now Rostekhnadzor), the situation with respect to nuclear security at Minatom facilities improved after the terrorist attacks of September 11, 2001, which elevated the priority of security concerns. Even so, the measures taken by the Russian government thus far have not yet filled all of the gaps in nuclear security. Vishnevskiy estimated that another $200 million would be needed to raise security standards sufficiently to meet federal requirements.[16] Since the total sum allocated to the special federal program comes to just over $250 million, the figure allotted for MPC&A maintenance and development (slightly more than 2 percent) will leave Russian sites woefully ill-prepared. For the time being, some major gaps are being filled in by foreign assistance and ad hoc funding, but the time has come for the Russian government to take over responsibility, committing the necessary funds in a transparent manner and on a sustained basis.

2.2 Aging Infrastructure

One of the most alarming problems facing Russia since the collapse of the Soviet Union and the initiation of economic reforms is the steady decline in the condition of the nation's industrial, nuclear, transportation, and military infrastructure. Despite the improving economy, the Russian government has few funds to refurbish infrastructure and no coherent plan for improvements, even when the funding does become available. According to some estimates, the depreciation of the capital stock in Russia has reached 60 percent–up to 75 percent in some sectors–meaning that these elements of the country's infrastructure are on the brink of collapse.[17]

In anticipation of possible disruptions, the Ministry of Emergency Situations and the Academy of Sciences have undertaken a survey of threats resulting from, among other things, the deterioration of industrial equipment and infrastructure. This study found that the worsening condition of Russia's 2,500 chemical plants, 1,500 facilities containing radioactive substances, 8,000 sites housing explosives, and 30,000 hydrotechnical structures held at risk a population of over 90 million people.[18]

The situation has serious repercussions for security at nuclear facilities. The equipment at these facilities is often inoperative because staffs lack the funds and expertise to repair it. The situation is even more alarming at defense nuclear facilities. At Mayak, for example, the depreciation of the infrastructure has reached 60 percent, while 35 percent of incidents are attributed to technical

15. "On the Special Federal Program 'Nuclear and Radiation Safety and Security of Russia for the Years 2002-2006,'" Government Resolution no. 149, February 22, 2000, <http://www.minatom.ru>.

16. Charles Digges, "Nuclear Materials Have Been Disappearing from Russian Nuclear Power Plants for Ten Years," Bellona Foundation Website, November 15, 2002, <http://www.bellona.org/ru/international/russia/nuke-weapons/nonproliferation/27273.htm>.

17. United Russia Duma Faction Website, <http://edin.ru/user/forum_read.cfm?id=20>.

18. "Ministry of Emergency Situations Will Release an Atlas of Threats and Risks for Russians," Newsru.com, November 7, 2004, <http://newsru.com>.

problems with equipment. The latter figure has another important meaning: The remaining 65 percent of incidents are therefore caused by human error.[19] Moreover, a great deal of the security equipment has been operating well beyond its service life.[20] The proportion of equipment that is five years old or less has declined dramatically, while the proportion of equipment that has exceeded its service life has increased.[21] When polled about the condition of security systems at their facilities, 29 percent of nuclear managers reported that security equipment was "sometimes" broken, while only 43 percent said that on-site personnel were capable of repairing inoperative or malfunctioning equipment.[22] Sites with Western-upgraded security systems are likewise plagued with sustainability problems. Few indigenous resources are available to maintain and repair the new security gear.

During the 1990s and until very recently, power outages at nuclear facilities were commonplace, shutting down equipment for hours at a time and rendering even state-of-the-art electronic security equipment useless. Outages presented such a threat that the Russian government issued a resolution forbidding electrical utilities to cut the power supply to strategic facilities. Local utilities often neglected to comply with this resolution, thus jeopardizing the safety and security of strategic facilities that failed to pay for their services on time. In some cases, nuclear facilities lacked the funds to pay their bills; in others, staff members themselves switched off the power on weekends to save money.[23] In addition, pilfering power transmission lines and other components and selling them for scrap has become commonplace. Between 2002 and 2004, for instance, scavengers disabled about 70 power transmission substations in the Urals region–the site of numerous nuclear facilities and other potential industrial hazards–alone. These scavengers typically target backup transmission lines, which are held in reserve for emergency situations. Needless to say, this imperils the safety and security of nuclear facilities in the region, which depend on a ready supply of backup power.[24]

Besides the obvious safety concerns aroused by such cases, there were serious security implications. Power interruptions could create the opportunity for thieves to remove nuclear or radioactive materials from a facility. Management and employees, for whom such interruptions have become routine, could fail to recognize a potential threat and to provide adequate protection. As Russia's economy has picked up over the last several years, such incidents have become rarer. However, nuclear facilities in more remote areas still remain vulnerable.

---

19. Nadezhda Kutepova and Vladimir Spivak, "Mayak's Debt May Reach One Billion in 2004," Antiatom.ru, <http://www.antiatom.ru/pr/pr040228.htm>.

20. "People and Equipment Are Tired: Economy on Security Hastens Technogenic Disaster," *Novaya Gazeta* 56 (August 5, 2002); "Hearings on Security at Russian Duma," *Yaderny Kontrol* 2 (March-April 1998): pp. 34-36. According to Vladimir Kuznetsov, a former chief inspector at GAN, 50 to 90 percent of equipment is operated beyond its service life. Vladimir Kuznetsov, *Main Challenges to Security at Nuclear Fuel Cycle Facilities* (Oslo: Bellona, 2002).

21. Yevgeniy Gavrilenkov, "Problem 2003: The Future of the Russian Economy and the Modernization of the Capital Stock," Report at a Seminar of the Center for Strategic Research, February 2003, <http://www.csr.ru/conferences/pr20003-2.html>.

22. Igor Khripunov, Maria Katsva, and Terrell Austin, "Establishing a Security Culture in Russia: Preliminary Findings," *The Monitor* 7 (spring 2001): pp. 10-14.

23. Matthew Bunn, "Loose Nukes," Interview with *PBS Frontline*, 1999, <http://www.pbs.org/wgbh/pages/frontline/shows/nukes>; "Loose Nukes Fears: Anecdotes of the Current Crisis," *Global Beat*, Issue Brief no. 45, December 5, 1998. For example, in the summer of 2002, the Scientific Research Institute for Applied Microbiology in Obolensk, whose inventory includes pathogens such as anthrax and the plague, was cut off from power supplies because of $1.7 million in unpaid bills owed to local utilities. Earlier in 2002, under similar circumstances, the leadership of the Institute instructed the staff to weld all exits and entrances shut except for the main one, where additional guards were posted. "Custodians of Anthrax and Plague Were Cut Off from Power Supplies," Strana.ru, August 15, 2002, <http://www.strana.ru>.

24. Nikolay Ivanov, "Metal Fever," *Nezavisimaya Gazeta*, November 1, 2004.

2.3 Federal System in Decay

The breakup of the Soviet Union contributed to centrifugal political tendencies within Russia itself during the early and mid-1990s. Following the famous policy initiative issued by President Boris Yeltsin, "Take as much sovereignty as you can handle," regional leaders used the weakness of the federal government to wrest considerable political and economic autonomy from Moscow. As a result, nuclear facilities became more dependent on the regional authorities for economic support. This trend did not affect sites of high national security significance to the same degree it did civilian organizations. Even so, the control exercised by regional authorities over communications, power supplies, and other infrastructure made it difficult for Minatom to maintain smooth operations.[25] In addition, the drop in federal budgetary subsidies to local economies resulted in a significant stratification of Russian regions. On the one hand, a small group of developed and resource-rich regions acted as donors to the federal budget, while on the other, a large group of regions was unable to perform even the basic functions of government without federal help.

Because nuclear facilities were increasingly dependent throughout the 1990s on the regional authorities to supply their infrastructure and workforce needs, and because they were located great distances from the headquarters of the industry, they sometimes came to feel greater loyalty to the region than to the federal center. Organizational and administrative disputes with regional governments sometimes went against Minatom, further reducing the ministry's influence on sites nominally under its jurisdiction. The distance of these sites from Minatom headquarters, coupled with the inability of Minatom to protect and support its own facilities, diminished incentives for facility management to strictly uphold and enforce industry-wide procedures and regulations, even as it tempted them to seek out foreign economic activity.

In the late 1990s, however, the federal government in Russia made a serious effort to counteract this centrifugal effect. The result was a steep decline in political and economic regionalization. Although residual effects remained, the vertical chain of authority was in essence restored. (Though they arguably undermined Russia's inchoate democratic institutions, the counterterrorist measures announced by President Putin in response to the Beslan hostage-taking situation in September 2004 tended to reinforce this centralizing process.) Minatom stepped up its effort to develop closer ties to regional authorities, ensuring that its facilities received proper attention and support from local governments. The ministry pledged to increase cooperation and other tangible benefits in the form of infrastructure development, employment, and higher living standards. To that effect, a number of cooperative agreements between Minatom and regional governments have been signed in recent years.[26]

One such Minatom initiative resulted in the establishment of the Union of Territories and Facilities of the Nuclear Energy Sector, an organization aimed at coordinating the efforts of Minatom and regional governments to address the social and economic problems in the regions, developing joint programs and projects, facilitating economic reform, and developing legislative initiatives for these purposes. The union currently includes 21 Russian regions, while another seven, including the city of Moscow, have expressed interest in joining.[27] Saratov regional governor Dmitriy Ayatskov, one of the more powerful regional leaders, currently heads the union, whose

25. There is extensive evidence of power being cut off from critical defense and nuclear facilities for non-payment of bills to the local budget, or as a result of theft of power lines by local criminal groups. Other evidence exists of repeated security-related incidents involving military personnel at nuclear and other weapons-of-mass-destruction facilities. These personnel typically attempt to steal valuable parts or equipment and sell it. See Newsru.com, December 11, 2003, <http://newsru.com/russia/11dec2003/steal_print.html> for more information.

26. For example see the official press release from Rosatom, Rosatom Website, May 26, 2004, <http://www.minatom.ru/presscenter/text.php?ssd=19166.txt>.

27. For more information on the Union, see its website, <http://www.atom-regions.ru>.

agenda also emphasizes nuclear security issues and antiterrorist preparations.

Despite the restoration of the vertical relationship between Rosatom and the sites, a partial breakdown of communication and infrastructure links between Rosatom headquarters and some nuclear sites, particularly those in remote locations in Siberia, the Arctic North, and the Far East, continues to be evident. In these cases regional elites have retained their clout, which they sometimes turn to purposes counter to those of Rosatom in their political dealings with the federal government.

2.4 Antisocial Behaviors

The nuclear industry has not escaped the social traumas of the transitional period in Russia. Indeed, these traumas have undercut the safety and security of nuclear-materials storage, transportation, and handling. Inadequate living conditions, low pay, and scant prospects for professional advancement have undermined the motivation of nuclear industry employees to perform their duties to high standards.[28] Economic difficulties have accelerated the spread of corruption, even at the highest levels, and increased the incidence of drug abuse and alcoholism among the workforce–including security personnel. Despite the facts that the Russian economy has shown signs of recovery for several years, and that some parts of the nuclear industry have become more productive, profitable, and better paid, the personnel situation has not improved fast enough to keep pace with the threat. These harmful phenomena, which are intrinsic to Russia's inchoate professional culture, significantly hamper the promotion of security culture.

2.4.1 Corruption and Crime

Despite numerous anti-corruption and anti-crime campaigns, the vigorous involvement of former and current law-enforcement and intelligence officials in politics and business, and the enactment of several anti-corruption and crime-fighting legislative and normative acts, Russia continues to be one of the most corrupt and crime-ridden nations in the world. In its annual studies of world corruption, an authoritative nongovernmental organization, Transparency International, has repeatedly ranked Russia at the bottom of almost 100 countries examined. It received scores ranging from 86 to 71, for a composite corruption score of between 2.1 and 2.7 on a scale of 1–10 (10 being the least corrupt).[29]

The most dangerous facet of this widespread corruption is its penetration of virtually all areas of politics, government, and the economy–including sensitive sectors such as law enforcement and the military that have a direct bearing on the security of nuclear materials. On September 4, 2004, in his address to the nation following the Beslan crisis, President Vladimir V. Putin acknowledged that "corruption has defeated the courts and the law enforcement services."[30]

At most nuclear facilities, security is provided by Interior Ministry troops, sometimes with the help of Rosatom's departmental guard force and other services under the supervision of the Federal Security Service (FSB). Corruption in the Interior Ministry has been officially acknowledged and has acquired dangerous proportions. A string of procedural breakdowns, for instance, let two female suicide bombers board planes at Moscow's Domodedovo Airport in August 2004, exposing once

28. For more information, see Institute of Sociology, Russian Academy of Sciences, and Greenpeace Russia, *Nuclear Energy Industry of Russia* (Moscow, 2003); Zhuravlyov, *From Theory to Practice*; Kuznetsov, *Main Challenges to Security at Nuclear Fuel Cycle Facilities*; Stephen White, *Russia's New Politics: The Management of a Post-Communist Society* (Cambridge: Cambridge University Press, 2000).

29. Data for the years 1996-2003. "Corruption Perceptions Index 2003," Transparency International Website, October 7, 2003, <http://transparency.org>.

30. Vladimir V. Putin, "Address of President Vladimir Putin, September 4, 2004," <http://www.kremlin.ru/text/>.

again the reality that bribery, extortion, and negligence pervade Russia's security systems. Many Russians consider their law-enforcement authorities to be as crooked as the criminals they are supposed to catch.[31] Before the Domodedovo incident, the innumerable everyday cases of police corruption received little attention. In 2003, foreshadowing the August 2004 airport debacle, a traffic police officer in southern Russia was convicted of corruption for letting through a truck that carried tons of explosives from Chechnya–the same kind of explosives that in 2000 had been used to bomb two apartment buildings in Moscow, killing several hundred people.[32] In the same way, a low-ranking police officer in Moscow was recently convicted of helping a group of future terrorists obtain residence papers in Moscow. The group took several hundred people hostage in a Moscow theater in October 2002.[33]

Nor are nuclear facilities immune to terrorist threats. In 2003, the FSB intercepted a suspected terrorist cell that was planning to strike at targets including the Kurchatov Nuclear Research Institute in Moscow.[34] In the aftermath of the Moscow theater hostage crisis, the FSB detained a captain of the security guard detachment at the Kalinin nuclear power plant who had in his possession a map of the facility and a coded list of telephone numbers. The phone numbers turned out to belong to individuals in Chechnya.[35]

Corruption in the armed forces can place weaponry in the hands of those who want to use it to carry out outside attacks on nuclear facilities. According to a former Russian interior minister, Boris Gryzlov, his troops confiscated an array of illegally acquired heavy weapons, including fully equipped tanks and multiple rocket launching systems (MRLS). These armaments had been obtained from legally established private enterprises. On at least two occasions, on August 28 and September 4, 2002, T-72 tanks with all of the standard armaments and "Smerch" MRLS were found in the possession of two private companies based in the Moscow region. In September 2002, Gryzlov announced that in 2001 alone his agency had confiscated about 1.5 tons of explosive substances and 9,000 explosive devices.[36]

Ironically, with the Beslan tragedy still fresh in Russians' memories, it was reported that the Moscow regional police had discovered a ton of plastit-type explosives stored virtually unprotected at one of the Defense Ministry's research institutes. These explosives were originally intended to be used for clearing minefields, but were later abandoned on the territory of the institute.[37] Such accumulations of weapons and explosives present a tangible threat to nuclear security. In the prevailing climate of corruption, a terrorist group could quietly procure everything it needed to launch an organized attack on a nuclear facility. Russia has yet to introduce a nationwide accounting and control system for weapons, ammunition, and explosives.

Corruption in the military, including among interior troops, has been aggravated by a deepening social and psychological crisis that envelops both the junior officer corps and rank-and-file conscripts. Morale in the officer corps has suffered from low pay, abysmal living conditions, the declining prestige of military service, and, most importantly, the lack of prospects for improvement. The military profession, which commanded prestige and material rewards during the Soviet era,

---

31. Peter Baker and Susan Glasser, "Russian Plane Bombers Exploited Corrupt System," *Washington Post*, September 18, 2004.

32. <http://www.polit.ru>, January 13, 2000.

33. "Who Hosted Terrorists," *Agentsvo Federalnykh Rassledovaniy*, September 28, 2004.

34. "A Suspected Terrorist Cell That Was Planning to Strike at Targets Including the Kurchatov Nuclear Research Institute Intercepted in Moscow," Newsru.com, August 11, 2003, <http://newsru.com/russia/11aug2003/shahid.html>.

35. "Captain of Security Guards at Kalinin NPP Is Suspected of Transferring Sensitive Information to the Chechens," Newsru.com, November 20, 2002, <http://newsru.com/russia/20nov2002/tverterakt_print.html>.

36. "Interview with Interior Minister Boris Gryzlov," *Interfax*, September 13, 2002.

37. "One Ton of Explosives Was Discovered on the Territory of a MOD Research Institute in Nakhabino," Newsru.com, September 6, 2004, <http://newsru.com/russia>.

now compares very unfavorably with the lifestyles and incomes enjoyed by the business elite, and even by the emerging metropolitan middle class. For conscripts the two-year term of military service has for some time amounted to a prison sentence. In addition to substandard food, poor living quarters and uniforms, and confinement to barracks for long periods of time, the soldiers have to endure hazing from both their peers and their commanding officers, who often use their units as cheap labor and find it convenient to take out their frustrations on conscripts—sometimes violently.[38] When inadequately skilled, demoralized interior troops bear most of the responsibility for physical security, improving security culture inside a nuclear facility is problematic at best.

Minatom has also experienced its share of corruption and crime. This malady extends to officials of all ranks and goes beyond the mere misappropriation of funds. In the fall of 2003, for instance, a deputy director of a nuclear fleet repair and maintenance facility in Murmansk was caught attempting to sell a suitcase containing 2kg of uranium isotopes 235 and 238. Other radioactive materials were also found in his possession. This material could have been used to manufacture a radiological, or "dirty," explosive device.[39] According to official Minatom statistics, there have been numerous attempts to divert nuclear and radioactive materials from Russian nuclear facilities since the early 1990s. The problem of corruption has focused the attention of President Putin, who was reelected in early 2004 with a solid mandate. Putin's 2004 inaugural address pointed to corruption as one of the central hurdles his administration intends to overcome.

2.4.2 Drug Abuse and Alcoholism

The use of illegal drugs and the rate of alcoholism among the Russian population have increased dramatically since the early 1990s. The increase is explained in part by the greater availability of drugs and alcohol. It also derives from the social and psychological problems that have bedeviled the population as a result of political turmoil, uncertain economic reform, and declining living standards. For all its faults, moreover, the Soviet system furnished moral and ideological structure. That structure has been shattered.

According to various estimates, drug use in Russia grew by anywhere from 400 to 800 percent from 1990-99. According to official information from the Interior Ministry, up to three million Russians use drugs regularly or occasionally. The figures for alcohol consumption are likewise alarming. Indeed, the Russian government convened a cabinet meeting in 2003 dedicated solely to this topic. Officially, the average Russian citizen–with the average including infants and the elderly–drinks the equivalent of 8.4 liters, or more than 2 gallons, of pure alcohol per year. Unofficial figures put the average at 14 liters, or four gallons.[40]

These ills have penetrated the nuclear industry. Although nuclear facilities with stringent security regimes and strict hiring procedures tend to have some immunity to these challenges, there have been persistent reports in the media about drug-related problems in closed nuclear cities, particularly Ozersk, and even among security guards, as at Sarov.[41] Similarly, there have been reports of widespread alcoholism among personnel at some nuclear facilities, notably the Leningrad nuclear power plant.[42] Minatom has vehemently denied all such accusations, pointing out that the accusers typically represent well-known radical environmental organizations that want

---

38. Five thousand military personnel in Russia commit suicide annually, more than die in combat in Chechnya. Almost 90 percent of draft-age youth are draft-dodgers. Michael Orr, "Chaos in the Barracks," *Wall Street Journal*, October 4, 2002.

39. "High-Level Official Was Detained in Murmansk While Trying to Sell Radioactive Materials," Newsru.com, October 2, 2003, <http://newsru.com/russia/02oct2003/mystery_man_print.htm>.

40. "Russian Cabinet Uneasy As Drinking Skyrockets," Russia's Johnson List, Center for Defense Information Website, February 19, 2003, <http://www.cdi.org/russia/johnson/7067-1.cfm>.

41. Vladimir Maryukha, "Guards Are Not Asleep," *Nuclear Security*, March-April 2000, <http://npi.iip.net/nucrep/n34-35/6.htm>.

42. Institute of Sociology, Russian Academy of Sciences, and Greenpeace Russia, *Nuclear Energy Industry of Russia*, p. 46.

to undermine the credibility of the nuclear industry. However, even the director of the Mayak facility at Ozersk admitted in his annual report that the situation with drinking on the job was getting out of hand. "I warn you," he pleaded, "if anything happens as a result of one of our employees being drunk on the job, we will be closed."[43]

The situation is worse at nuclear facilities that do not earn considerable outside revenues and thus subsist mainly on federal and Minatom budgetary allocations. According to an article in a Russian newspaper, the deputy mayor of the town of Lytkarino, the site of Rosatom's Scientific Research Institute of Instrumentation, was involved in the trade in both drugs and illegal liquor.[44]

The nuclear sector has not been spared the upheavals that have pervaded post-Soviet Russia. During the 1990s, the nation's transition to a new system of values and governance, accompanied by dramatically reduced budgets for the state-run nuclear sector, brought about a serious crisis in security arrangements for nuclear materials and radioactive sources. Rampant corruption and escalating rates of alcoholism and drug abuse, combined with severe funding shortfalls for MPC&A, have badly damaged the security culture within the nuclear sector.

Russian leaders privately acknowledge these problems and appreciate any help correcting them. The steady pattern of growth exhibited by the Russian economy since 2000, aided by soaring oil prices on the world market, may help lighten the burdens of providing adequate security infrastructure at Russian nuclear facilities and paying decent wages to personnel in the nuclear industry. However, newly available government revenues must navigate the Russian bureaucracy before they can fund improvements to MPC&A. President Putin has vowed to fight government corruption during his second term in office. Progress toward this elusive objective will have both a direct and an indirect impact on the security of nuclear materials in Russia.

Terrorist attacks in Russia and the United States have concentrated minds in Moscow, helping the nation better understand and fund its security needs. These developments are likely to pave the way for the emergence of a genuine nuclear security culture. Developing a security culture will be a time-consuming process, dependent on security perceptions among the national leadership, leaders' ability to manage their personnel at all levels, the amount of resources available to provide incentives, and a host of other factors. Subsequent chapters deal with the key components that will eventually contribute to Russia's nuclear security culture. They also chart a course to help improve this culture. ■

43. Institute of Sociology, Russian Academy of Sciences, and Greenpeace Russia, *Nuclear Energy Industry of Russia*, p. 48.

44. Georgy Zakaryan, "The Chechen Trap," *Moskovski Komsomolets*, October 20, 2000.

CHAPTER III

RUSSIAN LEADERS' PERCEPTION OF SECURITY

Russia makes a worthwhile case study for nuclear security culture because it belongs to a group of countries whose history, traditions, ongoing economic developments, and other traits complicate their ability to meet the standards of security culture discussed in Chapter I. This group includes transitional societies, countries whose nuclear programs lacked or still lack transparency, countries instituting nuclear power and research programs from scratch, and countries in which the nuclear industry is undergoing ownership reform. Russia falls into several of these categories.

Accordingly, this chapter focuses on the role of Russian national and regional leaders in shaping a security culture nationwide, and in particular at the organizational level.

In Western societies, leaders rely primarily on legal norms and time-tested management practices in the course of their daily work. In Russia, by contrast, leaders enjoy the leeway to do far more at their personal discretion. Thus the quality of individual leadership is far more important to the process of improving or degrading nuclear security culture in Russia than in the West.

Several reasons rooted in Russian history and tradition help explain this phenomenon:[1]

- *National mentality and traditions.* Russian political culture has traditionally combined collectivism and suppression of personal initiative with a high reliance on leadership. This makes a stark contrast with the individualism and personal initiative encouraged in the West. Throughout their history, Russians have not as a rule enjoyed the clear laws and detailed regulations found in Western society. The actions of the leader substituted for laws and other directives. The head of the Russian state, the tsar, was deified. He functioned not only as head of state but as the "God" and "Father" of the nation.[2] The authority and power of the head of state were unconstrained by any meaningful legal shackles. As former prime minister Mikhail Kasyanov noted, "Russia is the country which traditionally lives around the leader and with the leader."[3]

- *Autocratic society and the cult of personality during the Soviet epoch.* Totalitarianism, the "cult of personality," and the Communist Party dictatorship of the Soviet epoch reinforced the Russian tradition emphasizing the primacy of leadership. The remorseless suppression of individual freedom throughout Soviet society and the resulting social infantilism compelled leaders to play a more important role in Russia than in Western countries. The public for the most part played no part in decisionmaking. A recent survey of younger Russians–the generation that, ironically, is often portrayed as having a worldview that resembles that of the West–indicated that they believe mostly in God and the president.[4] A leading Russian political analyst, Gleb Pavlovsky of the Efficient Policy Foundation, said after the spring 2004 presidential elections that

---

1. For more information see William Dudley, ed., *Russia: Opposing Viewpoints* (San Diego, CA: Greenhaven Press, 2001); Timothy J. Colton and Robert Legvold, eds., *After the Soviet Union: From Empire to Nations* (New York: W. W. Norton & Company, 1992); A. Kuznetsov and N. Zakharov, "Specifics of Job Motivation in Russia," <www.znl.boom.ru.kuz.htm>.

2. Peter Lavelle, "Why Putin Tops the Polls," *Washington Times*, February 2, 2004.

3. Mikhail Kasyanov, "Russia Will Be a Presidential Republic for Another Ten Years," RBC News, March 14, 2004.

4. "Russian Youth Believes Only in God and Putin," RBC News, January 6, 2004.

> Russian citizens rely mostly on leaders to change their lives, rather than taking responsibility for changing their lives on their own.[5] When the Western media discuss the authoritarianism and dictatorship that supposedly characterize President Vladimir Putin's leadership, they generally agree that the public is interested in Putin more as a strong and charismatic leader than as the bearer of an attractive political program.[6]

It is not surprising, therefore, that in contemporary Russia, resource allocations and policy priorities depend as much on the leader as on laws and regulations, if not more so. In order to develop and improve the security culture within the Russian nuclear sector, leaders need to put more effort into the process by espousing the right values and creating an appropriate environment. This process will involve everyone from the country's top political leadership down to industry leaders and the managers of individual nuclear facilities.

3.1 National Level

The political leadership of the country includes the president and his staff, the executive branch, the legislature, and the regional elites.[7] (The judicial branch is covered in Chapter VII.) The roles played by the national leadership in the use of nuclear power, including the effort to ensure nuclear security, are defined by Section II of the 1995 Law "On the Use of Atomic Energy." A major problem with Russia's political structure, however, is that even a strong commitment at the top does not necessarily trickle down to the mid-level implementing authorities. For example, a 2002 report by the Main Inspection Directorate under the Office of the President revealed serious bottlenecks that impeded timely and complete execution of orders and directives within government ministries and agencies. Over 600 memoranda had to be dispatched in the first six months of 2002 to these agencies demanding corrective measures.[8] These bottlenecks are not unique to Russia, but they do pose serious impediments for a bureaucracy in flux. The series of administrative reforms launched by the Putin administration in March 2004 has yet to clarify matters or make officials more accountable for their actions.

In addition, tangled bureaucratic lines of authority make it difficult to coordinate security enhancement efforts. The "power ministries"–among them the Ministries of Defense and the Interior, the Federal Security Service (FSB), and the Foreign Intelligence Service–report to the president, while ministries and agencies such as the Federal Atomic Energy Agency (Rosatom), which exercises jurisdiction over most nuclear facilities, report to the prime minister. Nuclear security arrangements thus represent the combined efforts of multiple ministries and agencies with different chains of command and authority. Bureaucratic turf wars are a frequent result. These battles engender cynicism among government personnel and confusion among lower-level employees. Sen. Richard Lugar, who often travels to Russia to visit Cooperative Threat Reduction (CTR) sites, has testified to the poor interagency coordination in Moscow, which in turn complicates U.S. efforts to provide assistance. Sen. Lugar complained of receiving conflicting signals about CTR projects from "the President, the Foreign Ministry, the military, local commanders, and even local governments."[9]

---

5. Gleb Pavlovsky, "Russian Society Should Be Reformed," *Nezavisimaya Gazeta*, March 15, 2004.
6. Lavelle, "Why Putin Tops the Polls."
7. Under the Russian constitution, the president occupies a position above the three traditional branches of government.
8. Veronika Voskoboynikova, "Presidential Revisions Department Is Concerned with Implementation of the President's Orders," ITAR-TASS, September 16, 2002.

3.1.1 The President

According to Article 7 of the Law "On the Use of Atomic Energy," the president makes key decisions relating to the safety and security of nuclear facilities and approves guidelines that mold federal policy on the use of nuclear power. The Russian constitution places presidential authority somewhat above the authority of the three other branches of government–the legislative, executive, and judicial–thereby concentrating powerful leverage in his hands with regard to nuclear security. President Putin is on record declaring that nuclear security and nonproliferation represent two of his national security priorities.

A presidential document approved by Putin in December 2003, titled "Principles of State Policy on Nuclear Security and Radiation Safety in the Russian Federation for the Period Through 2010 and Beyond," declared that the president would provide general supervision and guidance on nuclear security and safety.[10] As noted above, however, muddled lines of authority will likely encumber the exercise of presidential power in these areas.

The document also lays out several factors that will determine Russia's nuclear security policy:

- an increase in the number of sites that contain nuclear materials and radioactive waste
- the need to reprocess or otherwise deal with the major quantities of nuclear and radioactive materials produced in the course of Russia's nuclear-weapons program and related programs
- the increased threat to nuclear facilities from domestic and international terrorist groups
- the impending obsolescence of physical protection systems and other security equipment installed at nuclear facilities
- the need to decontaminate vast territories left contaminated as a result of inefficiencies and errors of judgment made in the early stages of the Soviet nuclear program
- the significant growth of international cooperation in nuclear security and radiation safety
- the insufficient funding that has been provided for these purposes to date

For President Putin, the nuclear security agenda has acquired much greater significance, both domestically and internationally, because of acts of terrorism in Russia and in the world, plausible threats to Russia's national security from weapons of mass destruction, and his security-related past. His KGB background facilitates the president's understanding of security problems and helps him prioritize these problems within the decisionmaking process. Although under the 2004 administrative reform he initially demoted the Ministry of Atomic Energy (Minatom) to agency status, folding it into the Ministry of Industry and Energy, he later placed the agency under the direct supervision of the prime minister to rectify the situation.

President Putin has demonstrated his willingness to take a personal hand in rectifying problems with nuclear security. Following the August 2000 terrorist attacks in Moscow and the September 11, 2001 terrorist attacks in the United States, for example, the Federal Security Service, reportedly acting at the request of the Office of the President, unearthed several security breaches at nuclear facilities. In November 2001, President Putin requested a report from the newly appointed minister of atomic energy, Alexander Rumyantsev, about numerous security improprieties under

9. Richard Lugar, "Persistent Diplomacy Needed for Nonproliferation Advances," Address to the National Press Club, Washington, DC, August 11, 2004.

10. Office of the President, "The Principles of State Policy for Nuclear Security and Radiation Safety and Security in the Russian Federation for the Period Through 2010 and Beyond," Presidential Directive no. PR-2196, December 4, 2003, <http://www.scrf.gov.ru/Documents/Decree/2003/2196.html>.

his jurisdiction. The president was alarmed and was reportedly poised to take harsh measures; Rumyantsev argued that, after only a few months on the job, he could not be held liable for security problems that had bedeviled Minatom throughout the 1990s. He vowed to remedy the situation, and Putin reportedly kept an eye on his efforts.[11]

In response to the Beslan hostage-taking tragedy and previous terrorist acts, President Putin had to admit that his government "had stopped paying the required attention to defense and security issues and showed itself weak."[12] In addition, he issued directives mandating better interagency coordination among law-enforcement personnel, ordering the regional authorities to compile lists of hazardous sites requiring special protection, and attempting to enlist public support in the fight against catastrophic terrorism. Putin also evinced a keen interest in emulating the experience of the United States and other Western countries in restructuring the security and law-enforcement services to deal with new threats. At a cabinet meeting on September 13, 2004, he spoke in favor of establishing an integrated security system to provide comprehensive protection against terrorist acts.[13] These and other innovations allegedly designed to improve nuclear security elicited a mixed reaction in Russian society and the West, however, because of concerns for the resilience of democratic institutions in Russia. Some experts believe that Putin's initiatives had less to do with increasing Russians' security than with furthering the Kremlin's clout.

Putin's major tool for superintending security issues is the Security Council, a more or less exact counterpart of the U.S. National Security Council.[14] On June 7, 2004, the president signed a decree on the Statute of Russia's Security Council. This decree enhanced the role of the Security Council as a high-level, interagency advisory body to the president, who chairs its meetings, on matters of national security. On November 13, 2003, the president chaired a meeting of the Security Council and the Presidium of the Federal Council (which includes seven regional governors) and the public to consider how to better protect facilities vital to Russia's national security from terrorist and technogenic threats. Among other things, the meeting's agenda covered nuclear security. In December 2003, President Putin convened another meeting of the Security Council to discuss the nonproliferation agenda and consider how to improve the enforcement of security at sensitive sites. As of September 2004, the Security Council staff was reportedly at work drafting a new set of guidelines for combating proliferation and developing a new concept of national security.

Most observers believe, however, that the Security Council underperformed badly during the August-September 2004 series of terrorist acts. Some of these observers advocate upgrading the status of the council to that of a national coordinating body which can address important emergencies. For example, proponents of a more expansive role for the Security Council want the council's situation center to be retooled for continuous operations, allowing it to deal more swiftly with emerging threats. Such a reform would propel the Security Council into a leading role in nuclear security, alongside the government's 11 high-level interagency groups and the Science Council.[15]

Another option for President Putin to act in this domain is through presidential envoys in the regions.[16] Two envoys oversee federal nuclear weapons centers: Sergei Kirienko in the Privolzhskiy region (in Sarov), and Petr Latyshev in the Urals region (in Snezhinsk). They visit the sites under

---

11. Yuri Golotyuk, "Peaceful Atom and Martial Law," *Vremya Novostei*, November 12, 2001.

12. Vladimir V. Putin, "Address of President Vladimir Putin, September 4, 2004," <http://www.kremlin.ru/text/>.

13. Vladimir V. Putin, "Address of President Vladimir Putin to the Cabinet Meeting, September 13, 2004," <http://www.kremlin.ru/text/>.

14. Significantly, the abovementioned document "The Principles of State Policy for Nuclear Security and Radiation Safety and Security in the Russian Federation for the Period Through 2010 and Beyond" was developed by the Security Council and approved by President Putin.

15. Alexandra Samarina, Vladimir Mukhin, and Ivan Rodin, "Some Want to Give Clout Back to Security Council," *Nezavisimaya Gazeta*, October 20, 2004.

16. The practice of designating regional presidential envoys was instituted to coordinate and oversee the implementation of presidential policy in a given region. Envoys act on behalf of the president pursuant to his direct instructions.

their purview on a regular basis in an effort to bolster security arrangements at these sites and spur other improvements. In December 2002, Leonid Drachevskiy, formerly the president's envoy in the Siberian region, visited the Chemical and Mining Combine at Zheleznogorsk after the local security services detected severe security breaches. He discussed improvements with the management of the installation.[17] In February 2003, Latyshev and Security Council Secretary Vladimir Rushailo met with regional administrators and the managers of nuclear facilities to discuss the current situation and debate how to improve security and safety at these facilities. The newly appointed envoy Anatoly Kvashnin, a former chief of the General Staff, visited Seversk and the Siberian Chemical Combine in October 2004, proclaiming that the security of strategic facilities was a top priority for him.[18] In the Far Eastern region, the site of many nuclear facilities (mostly relating to submarines) and radioactive facilities, presidential envoy Konstantin Pulikovskiy has been raising concerns about the security and safety of sites and materials. Pulikovskiy regularly calls on the federal government to boost its assistance in the realm of nuclear security.

In view of Russia's historical background and its tradition of the primacy of individual leadership, the role of President Putin as a nuclear security advocate and role model is hard to overestimate. Russian political psychologists maintain that Putin had achieved an almost "sacral" status with the Russian populace as he began his second term in office. In short, it is of little consequence to Russians what the president says or how he says it; it is simply important that it is he who says it.[19] In the post-Beslan period, when the electorate might have held the president partly responsible for the debacle, Putin's job-approval ratings and credibility hardly budged. From this some experts concluded that, absent any other leader to defend Russians physically and psychologically, and absent any viable political challenger to Putin himself, Russian society would continue to rally around the president.[20] In September 2004, asked to state which institutions they trusted most, Russians ranked the president first (56 percent), followed by the church (43 percent) and the armed forces (30 percent).[21]

3.1.2 Government/Cabinet

Putin has demonstrated a level of commitment to nuclear security and antiterrorism that figures to act as a catalyst for the emergence of a security-conscious mentality. Despite the president's personal focus on security, however, his influence is diffused somewhat when it comes to conceiving of specific initiatives and pushing them through Russia's government bureaucracy. There has clearly been a disconnect between Putin's declarations and commitments, on the one hand, and the persistent inadequacy of Russia's nuclear security arrangements, on the other. The disparity between promise and performance results from insufficient funding and the low priority traditionally accorded these arrangements. Despite the far-reaching powers granted him under the Russian constitution, Putin has failed to use his clout to clear the bureaucratic obstacles to more effective Western assistance in the area of nuclear security.

In accordance with Article 9 of the Law "On the Use of Atomic Energy," the Russian government approves key documents relating to nuclear security and material protection, control, and accounting (MPC&A). Other functions discharged by the government include developing and managing the implementation of special federal programs, managing federally owned nuclear and

---

17. "Two Planted Bombs Remained Unnoticed at a Strategic Nuclear Facility," *Izvestia*, December 24, 2002.

18. Press Release, October 11, 2004, Rosatom Website, <http://www.minatom.ru/News/Main/viewPrintVersion?id=6585&idChannel=71>.

19. Interview with Prof. Elena Shestopal, political psychologist from the Moscow State University, February 17, 2004, <http://www.strana.ru/print/207738.html>.

20. ROMIR Monitoring, Public Opinion Poll, September 16-21, 2004, <http://romir.ru/socpolit/socio/09_2004/president1.htm>; "Interview with Igor Bunin, Director General of the Center for Political Technologies," *Izvestia*, September 6, 2004.

21. "Most Russians Are Happy in One Way or Another About Their Life," *Interfax*, October 2, 2004.

radioactive materials, making decisions about the construction, operation, and decommissioning of nuclear facilities, ensuring the physical protection of nuclear materials and facilities, and coordinating international cooperation in the nuclear area. In February 2000, for instance, the cabinet adopted a special federal program titled "Nuclear and Radiation Safety and Security of Russia for the Years 2000–2006," which laid out a strategy to protect nuclear facilities and develop a state system for the accounting and control of nuclear materials. As mentioned previously, the total funding originally proposed for the program through 2006 was $254 million, of which $202 million was to come from the federal budget and the rest from extra-budgetary sources. Only $5 million was originally earmarked for security.

In 2000, two cabinet meetings were held to deliberate on MPC&A matters. Members of the cabinet discussed funding, structural changes, a redistribution of functions, and interagency coordination. They approved a proposal to accelerate the development of the regulatory and legal framework for MPC&A. Funding was increased as a result of these meetings, but it remained insufficient. Minatom was allocated only $177,000 for material control and accounting (MC&A) work in 2001, and that meager sum fell to $111,300 in 2002.[22] International assistance continues to make up a large share of overall spending on physical protection, accounting for between 30 and 50 percent of the total.[23]

The December 2003 statement of "Principles of State Policy on Nuclear Security and Radiation Safety and Security in the Russian Federation for the Period Through 2010 and Beyond" admits that the funding provided so far for nuclear security is "insufficient" (Section II.6). Adequate funding is a prerequisite for both a technologically sophisticated security regime and an adequate nuclear security culture. If the federal government continues to issue grand pronouncements about security while failing to match its words with funding, the personnel who operate Russian nuclear sites will conclude–reasonably–that security culture remains of minor importance. The atomic energy minister was the traditional driving force in the interagency process, lobbying for more federal funding for the nuclear sector. In March 2003, speaking to deputies from the State Duma, Alexander Rumyantsev surprised many Russian observers by committing $200 million to improve physical protection at Russia's nuclear sites over the next six years. Now that Minatom has been demoted from a ministry to an agency, however, it is hard to say whether Rumyantsev will be able to deliver on this commitment. Even if he does, $35 million per year, while a substantial sum of money by Russian standards, is unequal to the myriad security problems plaguing the nuclear sector.[24]

Because of divergent and conflicting funding priorities among its members, the Russian cabinet faces many difficult choices. Nuclear security hardly tops the list of priorities. The cabinet usually turns its attention to these issues only when media reports expose embarrassing problems, terrorist attacks pose a credible risk, or a foreign government voices concerns about nuclear security breaches in Russia. Prodded by the president or acting under international pressure, the cabinet sometimes takes nuclear security issues quite seriously, but this attitude is more sporadic than long-term and consistent.

A good illustration of this proclivity to appease the West rather than acting out of a sense of Russia's own security interests came during Defense Minister Sergei Ivanov's visit to the United Kingdom in July 2004. In an address delivered during his trip, the minister announced a major test

---

22. Russian Ministry of Atomic Energy, *Work Plans for the Development and Implementation of the System of State Control and Accounting of Nuclear Materials*, April 9, 2001 and April 12, 2002. Obtained through an interview by the authors with a Rosatom official, January 16, 2003.

23. International Business Relations Corporation, "Foreign Trade Policy and Authorized Foreign Trade Entities of the Ministry of RF for Atomic Energy," *IBR Report* (Moscow, 2003); "Concerning Internal Troops of the Ministry of Internal Affairs of the Russian Federation," Federal Law no. 27-FZ, February 6, 1997, <http://www.referent.ru>.

24. Galina Filippova, "It is Planned to Channel 6.5 Billion Rubles to Protect Nuclear Facilities from Unauthorized Access," *RIA Novosti*, March 5, 2003.

of security at Russia's nuclear facilities and invited NATO countries to send observers. According to Ivanov, Moscow's main motivation in this show of openness was not to improve security but to silence Western critics who "question whether the Russian military's nuclear installations are safe from terrorists."[25]

Records show that publicly engaging Russia in a productive and balanced dialogue regarding nuclear security can pay off by inducing the media to focus on these issues, thereby prompting the leadership to respond. One example was the G-7 Nuclear Safety and Security Summit in Moscow in April 1996, which helped Russia demonstrate strong international commitments and concerns in this area. Each similar event can potentially add an important brick to the edifice of a Russian security culture. A more recent example took place during the summer of 2004, when the heads of the G-8 nuclear regulatory agencies convened in Moscow. Amid Putin's confused campaign to reform Russia's executive branch, this forum issued a clear call for an independent regulatory body to oversee security.

The Beslan tragedy was a wakeup call to the Russian government. Even before the string of terrorist acts in August-September 2004, the government had planned to increase defense spending by 28 percent over the 2004 level. Funding for internal security and law enforcement was to rise by 26 percent.[26] The Treasury has promised more money for antiterrorist measures, now called the country's no. 1 priority, for FY2005. As a result, as much as one-third of Russia's federal budget will be spent on defense, security, and law enforcement. In the absence of any meaningful breakdown of the budget, however, it is virtually impossible to determine the extent to which the nuclear security budget will be expanded under the antiterrorist funding. If it had raised the budget significantly and in a transparent manner, the government would have signaled its determination to deter and defeat any malicious acts involving nuclear material and the associated facilities. A larger, more transparent budget would also impress upon the nuclear workforce the importance of its professional endeavors and, in turn, engender a higher standard of security culture.

Rather than tapping the federal budget, which has benefited from a rapid rise in oil and gas revenues, the Russian government seemingly expects the international community to further increase its contributions. This attitude runs counter to the "Principles of State Policy on Nuclear Security and Radiation Safety and Security," which stipulate that Russia should end its dependence on other countries with regard to funding nuclear security. Since Rosatom and Rostekhnadzor are now directly responsible to the prime minister, the personal attitude of the latter towards security is very important. Although Prime Minister Mikhail Fradkov was first deputy head of the Security Council in 2000–2001 and worked for the security services in the 1970s, his background is mostly in trade. Security issues do not seem to rank high among his priorities. In 2004, for instance, he officially supported a Rosatom-promoted proposal to import spent nuclear fuel into Russia for storage and reprocessing. His advocacy of this concept, voiced at an international conference in Russia, ignored the hostility toward the idea evinced by experts and nongovernmental organizations that have decried Russia's inadequate infrastructure and its poor safety and security record.[27]

3.1.3 Parliament

Parliamentary functions in the area of atomic energy are defined by Article 8 of the Law "On the Use of Atomic Energy." These functions include enacting federal laws, approving special

25. "Russia to Stage Nuclear Security Exercise," Voice of America, July 13, 2004. The exercise, involving transportation of nuclear weapons, took place as planned in August 2004 with all parties participating, including NATO observers. Ivanov and Rosatom Director Alexander Rumyantsev reported the results to President Putin, who promised to remain personally involved in nuclear security issues.

26. The 2005 budget, including these figures, had been approved by the State Duma by the end of September 2004. *Nezavisimaya Gazeta*, September 29, 2004.

27. "Mikhail Fradkov Considers Russia the Best Place for Burial of Nuclear Wastes," Lenta.ru, June 27, 2004, <http://www.lenta.ru>.

federal programs and budgets, and holding public hearings. Members of parliament can request information of the government and can summon the heads of agencies or other government officials to respond to questions during the "governmental hour," a meeting held periodically for this purpose. To invite a government official to participate in this discussion, a member of parliament forwards a request through the speaker of one of the chambers of parliament (usually the Duma), who assigns a committee to arrange the meeting. After the meeting is held, parliament can follow up in several ways, for instance by requesting the president or the cabinet to take action or by initiating legislation.

At present the Russian parliament lacks the authority enjoyed by most parliaments to control and oversee the implementation of government policy (although it is considering a bill to that effect). Even if adopted, however, the bill under deliberation would provide only limited oversight authority, giving lawmakers the ability to investigate emergency situations or severe violations. This would pale in comparison to the prerogatives of, say, the U.S. Congress. Although its influence on the enforcement of nuclear security would likely be negligible, the new law could represent a step in the right direction.

Under the impact of the Beslan tragedy, President Putin made an exception to the practice of excluding parliament from policy. He agreed to establish a joint Duma-Federation Council commission to investigate the hostage-taking situation, waiving the normal procedure for debating and approving the bill. The inquiry remained under the control of lawmakers loyal to the government, and the Federal Assembly rejected proposals to add independent deputies to the commission and to open its work to public scrutiny. Skeptics characterized the commission as a public-relations gimmick unable to produce an independent and in-depth study.[28] Nevertheless, the inquiry set an important precedent by allowing the legislature to look into sensitive government policies and their implementation.

In Russia individual members of parliament, rather than political parties, have typically called attention to nuclear security issues. The "Yabloko" party was one exception to that pattern. Yabloko raised concerns about nuclear security and questioned whether the current system was adequate to prevent diversions of sensitive materiel or acts of terrorism. The most charismatic champion of nuclear security in the State Duma was Yabloko Deputy Chairman Sergei Mitrokhin. In 2002, Mitrokhin, accompanied by a group of journalists, made a successful, well-publicized attempt to gain unauthorized access to a nuclear facility, the Chemical and Mining Combine at Zheleznogorsk, without being detected or stopped. The journalists shot a documentary of their incursion as evidence. In his follow-up campaign Mitrokhin demanded an investigation of the case, as well as an independent assessment of the facility's security system. The resulting uproar induced the regional FSB office to get involved, and to conduct its own test of security systems. FSB officers managed to plant a dummy explosive device at a spent-fuel storage facility.[29] Mitrokhin thus became one of very few persons in parliament to spotlight deficiencies in nuclear security.

The Yabloko party, however, failed to surmount the 5 percent threshold in the December 2003 elections and is no longer represented in parliament. It appears that the current legislature, which is more conservative and loyal to the government, will be reluctant to challenge the government on such sensitive issues. Now that Mitrokhin is gone, moreover, few members of parliament are likely to champion nuclear security.

The law has also been a matter of some contention. In the past there were some serious controversies between parliament and the president, including some related to the evolving

28. "Federation Council Sets Up a Commission to Investigate the Beslan Tragedy," Newsru.com, September 10, 2004, <http://www.newsru.com/russia>.

29. Andrei Yegorov, "A Bomb for Chemical and Mining Combine," Nuclear.ru, April 13, 2004, <http://www.nuclear.ru>.

nuclear legal basis. In 1999, for instance, after numerous unsuccessful attempts, parliament finally approved a law on nuclear weapons, only to have the bill rejected by the president on purely legalistic grounds. Had the president signed the bill, Russia would have been better equipped to streamline its nuclear security arrangements and clarify the roles of different actors. Failing such legislation, parliament will remain peripheral to the effort to improve nuclear security.

The acts of terrorism in August-September 2004 caught Russian legislators off-guard, exposing serious gaps in national law. In a rush of activity, deputies from the Federal Assembly initiated a series of amendments to existing laws and draft laws. Motivated by emotion, the deputies drew up these amendments in haste. Predictably, the substance of many of them was somewhat misplaced. In late September 2004, the Duma voted overwhelmingly for a resolution calling for sweeping improvements in security. The resolution, which outlined a legislative agenda but did not itself include any new laws, called for giving security agencies more powers and tightening security measures on subways and railways, at airports, and at other sites that might be targeted, including dams and nuclear power plants.[30]

Russian legislators are in the initial stages of developing a new legal basis in response to terrorist threats. To accomplish their mission, they need more expertise and information sharing with their colleagues in other countries, primarily the United States. Such cooperation would help them refocus their legislative efforts on vital, long-term issues such as nuclear security.

3.2 Regional Level

3.2.1 Regional Elites

This category includes governors, regional and local administrations, and members of regional legislatures. Article 12 of the Law "On the Use of Atomic Energy" authorizes regional and local authorities to participate in decisionmaking regarding public outreach, environmental protection, and the construction and operation of nuclear facilities. The Law provides regional elites with only a limited mandate to superintend nuclear security, even though they are clearly key stakeholders.

Regional elites generally view nuclear facilities on their territory as a source of additional revenues, prestige, and high-tech employment. These facilities generate funds through assistance from the federal government and international institutions, as well as through contracts with foreign partners.[31] Consequently, most regional administrators and lawmakers want to further develop the nuclear infrastructure while assuring its safety and security. The approach of the federal government is formulated as "rational combination of federal and regional interests in ensuring nuclear and radiation safety and security with the federal interests enjoying the priority."[32]

Well-established lines of communication link the regional and local governments with nuclear facilities on matters of security. Assistance from regional governments can take the form of direct financial allocations for nuclear security, tax breaks, or requests to regional representatives in the Federal Assembly to work to improve nuclear security and secure the necessary federal funding. Some regional governments have established coordinating councils to support federal antiterrorist and anti-crime efforts touching nuclear facilities. At the same time, the regional authorities are at the forefront of dealing with anti-nuclear movements and campaigns whose actions could pose a

30. Steven Lee Myers, "Russians Crack Down on Security Breaches," *New York Times*, September 23, 2004.

31. For example, cities where federal science centers are located are authorized to spend 20 percent of their total federal tax liability within the city rather than paying it to the federal treasury. Nuclear fuel-cycle facilities represent a substantial revenue source. Closed territorial entities (ZATO) are exempt from federal taxes and supported through federal programs in accordance with annual federal budget laws and "On Closed City Entities (a.k.a. ZATO)," Federal Law no. 3297-1-FZ, July 14, 1992.

32. Office of the President, "Principles of State Policy for Nuclear Security and Radiation Safety and Security."

threat to nuclear security. Regional authorities have increasingly sided with Rosatom and its policies, but there have been some exceptions, especially when federal policy was perceived to infringe on local and regional interests.

In order to keep the regional authorities informed and proactively involved, Rosatom has been actively working with the Council of Nuclear Power Territories and Facilities, a body headed by Saratov regional governor Dmitriy Ayatskov. Although the activities of the council focus primarily on economic and social improvements to the regions in which nuclear facilities are located, safe and secure operation of these facilities ranks among the most important issues discussed at its meetings.

As a result of the post-Beslan policy changes, regional elites are likely to be even more closely integrated into antiterrorist activity and into the protection of sensitive sites on their territory. Indeed, in their capacity as chairmen of regional interagency commissions, governors have been put in charge of coordinating responses to terrorist and other threats. Interior Ministry officers have been assigned to regional governments in the capacity of first deputy, helping them perform this function. These military officials have sweeping powers, enabling them to field a quick and effective response and coordinate the use of troops under the jurisdiction of other ministries and agencies.[33]

3.2.2 The General Public

The Russian general public has remained largely untapped and ill-informed in the campaign to strengthen and promote nuclear security. Public opinion, for example, ranks the risk of nuclear-material theft or diversion well below environmental degradation. Only a quarter of the Russian population considers nuclear proliferation to be a national security concern. A sizeable 16 percent of the public even supports the idea that Russia has the right to transfer nuclear weapons and technologies to other countries.[34] As late as July 2004, a Russian weekly published an article, evidently by an expert of nationalist convictions writing under a pen name, attacking a fellow expert for his pro-Western views on security. The author claimed that "proliferation problems among sovereign states are irrelevant to Russia." By the same token, "not only does a nuclear North Korea not pose any threat to Russia, it is rather beneficial" to Russian interests.[35]

One reason for this apparent apathy is that the public has little access to reliable information about the status of nuclear materials. Another is that nuclear security and proliferation are perceived as bound up with domestic politics and, in any event, too abstract to affect ordinary citizens. Most people do not fully grasp the meaning of the term "proliferation," and do not connect it with their everyday lives. Thus, although over 80 percent of the public considers nuclear diversion a possibility, this figure should be interpreted not as a sign of public alarm about the danger but as an acknowledgement that diversions are possible in a country where corruption and theft are commonplace. A pervasive negative or indifferent attitude towards the United States is another factor: Russians tend to view nuclear security and nonproliferation not as Russian national security imperatives but as an expensive, U.S.-imposed burden.[36]

In the post-Beslan period, moreover, many Russians have tended to impute malign intent and double standards to Washington's conduct toward Russia. President Putin implicitly alluded to this

33. Vladimir V. Putin, "Address of President Vladimir Putin to the Cabinet Meeting, September 13, 2004," <http://www.kremlin.ru/text>.

34. Center for Policy Studies in Russia, "Russians on Nuclear Weapons and Nuclear Threats," PIR-Center Report, 2000, <http://www.pircenter.org/data/publications/poll.pdf>.

35. Sergei Kremlev, "Dangerous Realities of Global Stability," *Nezavisimoe Voennoe Obozrenie*, July 23, 2004.

36. Authors' interviews with nuclear industry employees, 2000-2003. For more information see also Irina Koupriyanova, "Assessment of Effectiveness of U.S. MPC&A Assistance to Russia," *Yaderny Kontrol* 2 (March-April 2002): pp. 57-65; Vladimir Kuznetsov, *Main Challenges to Security at Nuclear Fuel Cycle Facilities* (Oslo: Bellona, 2002).

in his address to the nation on September 4, 2004, when he referred to dark and mysterious forces that sought to weaken Russia and feared its nuclear weapons. These comments loosed a torrent of anti-Western and especially anti-American commentary in the Russian media. In an early October 2004 public opinion poll, for example, 68 percent of respondents acknowledged that Russia had external enemies. Twenty-five percent specifically referred to the United States as a country that could initiate a war against Russia.[37] The subtext of much of this commentary came down to an desire to scapegoat nonexistent enemies, distracting from the failure of the Russian security and intelligence forces to counteract terrorist threats.[38]

Even so, public attitudes may be changing. President Putin recognized that the public can play an important role in promoting and strengthening security. In a series of directives issued after the August-September 2004 terrorist acts, the president instructed law-enforcement agencies to involve the public more closely in the effort to address security issues. In a major innovation, one directive created a "public chamber" to enhance the role of the public in considering and screening new, mostly security-oriented, legislative acts. It is too early to say how effective this initiative will be at transforming Russia's traditionally secretive society and making the public voice heard. Russia's leadership must understand that restraining democratic institutions and curtailing transparency as part of the ongoing antiterrorist campaign will likely undercut any efforts to enlist popular help in countering new threats and supporting security culture.

Although a number of nongovernmental organizations (NGOs) were established in Russia in the 1990s to deal with nuclear safety and environmental protection,[39] and although certain forms of government outreach were developed, little effort went into extending this outreach to nuclear security. Nuclear security was at once too sensitive a topic and too remote from daily life to arouse much popular interest. Now, however, the escalation of terrorism, the threat of sabotage at nuclear facilities, and the likelihood of theft or diversion of nuclear materials for use by terrorists have created an auspicious political climate to promote public security awareness.

The public can be made aware of the importance of nuclear security in two ways: (1) by imprinting on the popular mind the connection between environmental safety, a matter of public concern since the Chernobyl incident, and the security of nuclear and radioactive materials, and (2) by making the link between nuclear security and the growing terrorist threat. If citizens understand the importance of nuclear security, they will be more likely to:

- report attempts at diversion and terrorism
- report inadequate security perimeters, suspicious people near a facility, or other conditions that could contribute to a breach of security
- call media, government, and legislative attention to security problems at nuclear facilities
- form advocacy groups to elevate nuclear security on the government's list of priorities and bring it to a national audience through publications and public action
- understand the importance of adequate funding for nuclear security when issues of funding and distribution are discussed

---

37. "Russians Identified Their Country's External Enemies," Newsru.com, October 10, 2004, <http://newsru.com/Russia/>.

38. Andrew Kuchins and Dmitri Trenin, "Two Tragic Septembers," *Moscow Times*, September 24, 2004.

39. One of the most recent signs of public concern over nuclear safety was the active campaign to stop the production of mixed-oxide (MOX) fuel at the Siberian Chemical Combine. The campaigners were successful in attracting the attention not only of the leadership of the facility, but also of Rosatom itself. See "Naked Emotion and No Common Sense," Open Letter of the Leadership of the Siberian Chemical Combine concerning Say No to MOX!, the public action in the Tomsk region. Rosatom Website, <http://www.minatom.ru/News/Main/viewPrintVersion?id=8338&idChannel=366>.

Public support is important to enable the regional elite to pursue its policies on nuclear security. First, these officials are accountable to the public and need to keep the voters informed both about problems and about achievements in this area. Second, the public can be a valuable ally for the regional authorities by helping attract the attention of the media and the federal government to security issues. Thus, it is in the interest of the regional authorities to cultivate public knowledge about the value, risks, and initiatives associated with the nuclear sector.

This chapter sketches a mixed picture of the attitudes of the national leadership and the public toward nuclear security, and of the roles various actors can play and are playing in this process. The president's declaratory commitments often run afoul of bureaucratic politics in the executive branch. Even if the government spends more money to boost security, this will not necessarily raise security standards unless fundamental organizational and structural changes are introduced. The capacity of the legislature to foster nuclear security has dwindled from an already low level. Regional elites are engaged in the problem of nuclear security to only a limited degree. Finally, the public remains indifferent, although it has great potential to contribute to security. Unless these actors modify their perceptions and work together, higher standards of security culture will remain elusive. It remains to be seen to what extent the post-Beslan directives and resolutions will be implemented and whether they can improve the overall picture. ■

CHAPTER IV

NUCLEAR INDUSTRY FRAMEWORK

4.1 Industry Leadership

The bulk of Russia's nuclear sector, operated until recently by the Ministry of Atomic Energy (Minatom), has traveled a difficult and bumpy road. After inheriting the massive Soviet nuclear infrastructure, Minatom struggled throughout the 1990s to cope with the decline of the industry into decrepitude, not to mention Russia's centrifugal tendencies (see discussion in Chapter II), only to lose its prestigious ministry status and be downgraded to an agency (Rosatom) in 2004. This poorly managed evolution could not help but undercut the morale of nuclear personnel, and in turn standards of security culture.

As specified by Presidential Decree no. 314 "On the System and Structure of Federal Executive Bodies," issued on March 9, 2004, Minatom's functions were scaled back, and it was placed under the jurisdiction of the newly created Ministry of Industry and Energy. With respect to nuclear facilities, the Ministry of Industry and Energy assumed responsibility for policymaking, developing the legal basis pertaining to nuclear activities, developing and submitting budget requests to the government, and coordinating the distribution of federal funds among its constituent agencies. This presidential decree came as a shock to Russia's nuclear elite because it stripped Rosatom of all authority except for policy implementation and property management. However, the subsequent Presidential Decree "On the Structure of Federal Executive Bodies," issued on May 20, 2004, reversed what many Minatom veterans viewed as a humiliating course, making Rosatom directly responsible to the prime minister. The new decree also restored some of Minatom's prerogatives.

Rosatom kept as one of its four deputy directors Anatoliy Kotelnikov, formerly a deputy minister of Minatom in charge of protecting information, nuclear materials, and facilities. Serving at the rank of general, Kotelnikov once headed up the Federal Security Service (FSB) office in Yaroslavl oblast. The FSB has a mandate under law to ensure the security of nuclear facilities. Kotelnikov was one of the FSB officers who were routinely assigned to the Minatom (now Rosatom) headquarters staff or to individual facilities in the field to perform a variety of security functions. To have one of four deputy directors–the maximum permitted under the administrative reform–focus exclusively on security is certainly a luxury for this ministry-cum-agency. On the one hand, this arrangement could carry advantages in terms of streamlining, improving, and prioritizing security policies. On the other, FSB personnel still seem rather cautious and ambiguous about the notion of security culture, which they regard as an approach that is less tangible and time-tested than the military-style enforcement they know and trust. Indeed, military-style discipline worked effectively in the past totalitarian environment and could be a useful tool in the transitional period. However, there are grounds to believe that a transparency-oriented security culture would be easier to introduce in an organization led by civilians rather than FSB officers. This is particularly true now, when nuclear security culture is being applied to a much wider range of organizations and facilities. Even sites that are primarily defense-oriented are undergoing conversion to civilian uses, militating for a less regimented approach.

Rosatom accelerated the development of contingency planning in the post-Beslan period, in an effort to better protect nuclear facilities against terrorist threats and industrial accidents.

In an important conceptual breakthrough, Rosatom began urging the cabinet to group physical protection with antiterrorist measures, and to give this combined category special priority in terms of federal funding.[1] If adopted, this change would open up new channels for interagency communication, tap additional resources, and elevate the importance of nuclear security on the national agenda.

For the time being, however, jurisdictional issues are complicated because Rosatom facilities that operate as part of Russia's nuclear-weapons complex are responsible both to Rosatom and to the Ministry of Defense (MOD). The new MOD statute empowered the Defense Ministry to exercise oversight over nuclear security throughout the process of developing, manufacturing, testing, operating, storing, and disposing of nuclear weapons and military nuclear power plants and installations.[2] On August 9, 2004, Defense Minister Sergei Ivanov and Rosatom Director Alexander Rumyantsev reported to President Putin that they had developed a draft memorandum of understanding spelling out joint responsibilities for nuclear security at these sites. This document will probably remain classified, but it is possible to venture an educated guess as to its content. A likely scenario is that MOD, as a ministry that reports directly to the president, will be more visible at sensitive military facilities, while Rosatom remains in charge of civilian facilities. If so, confusion could ensue with respect to the security of nuclear materials over which both MOD and Rosatom can assert jurisdiction. Adding to this organizational confusion, facilities that implement both defense and civilian projects will likely retain their dual character in matters of security. Unless these problems are streamlined and smoothed out by amendments to the reform decrees, the new system will work against common and compatible standards of security. In the past, jurisdictional differences provided Minatom with a convenient excuse to deny inspectors from the Federal Nuclear Oversight Agency (Gosatomnadzor, or GAN) to projects and facilities that could be portrayed as defense-oriented. For instance, spent submarine fuel was transported at some point in the late 1990s in defective containers, but GAN was kept out under this pretext.

As was the case before the administrative restructuring commenced, MOD will continue to use its own personnel to regulate and oversee defense projects, while the newly established Federal Service for Environmental, Technical, and Nuclear Oversight (Rostekhnadzor), which now combines several jurisdictional areas, is expected to play a similar role for civilian projects. On the one hand, expanding the service and merging several nonmilitary regulatory and oversight services under a single head–the former GAN was folded into it–represents a welcome change. The new service is larger, answers directly to the prime minister, and thus wields more influence. On the other hand, the former Nuclear Oversight Agency is the smallest of the three components of Rostekhnadzor and thus might find its interests subsumed within the new body's larger agenda. The good news is that Andrey Malyshev was appointed acting director of Rostekhnadzor. Malyshev, a former deputy minister at Minatom and director of GAN, is likely to defend the interests of the nuclear sector. It bears repeating that monitoring and inspections by an independent oversight agency are a crucial factor in a healthy security culture.

In the meantime, as specified by the Statute of the Federal Atomic Energy Agency, adopted by Government Resolution no. 316, June 28, 2004,[3] Rosatom is responsible for:

- drafting legal documents relating to the material control and accounting (MC&A) of nuclear materials and radioactive sources, and enacting procedures, subject to cabinet approval

1. "Statement by Rosatom Deputy Director Anatoliy Kotelnikov at a Seminar on Physical Protection," *AtomPressa* 44 (November 2004), <http://www.minatom.ru>.

2. Office of the President, "Concerning the Ministry of Defense of the Russian Federation," Presidential Decree no. 1082, August 16, 2004, <http://www.refererent.ru>.

3. "Statute of the Federal Atomic Energy Agency," Government Resolution no. 316, June 28, 2004.

- drafting legal and normative documents regarding the MC&A of foreign nuclear materials on Russian territory, subject to government approval
- developing forms for nuclear-materials MC&A status reports to federal inventories, along with procedures for using and filing these forms
- developing procedures for certifying equipment at nuclear power plants
- developing procedures for certifying managers at nuclear facilities
- issuing import certificates assuring the peaceful use of nuclear materials, technologies, and power plants and setting the terms for re-exporting these items
- developing procedures governing (1) the physical security of nuclear facilities and institutions; (2) the relationships among departmental guards, the regional security services, and Interior Ministry troops; (3) the relationships among facilities, institutions, and organizations; and (4) recovery from accidents that take place while nuclear and radioactive materials are being transported
- assuring compliance with international nuclear-materials physical protection norms and International Atomic Energy Agency (IAEA) requirements governing nuclear security

Rosatom has numerous direct channels of communication with the IAEA and is represented at IAEA headquarters in Vienna. Russia is party to the Convention on the Physical Protection of Nuclear Material, the Nuclear Safety Convention, the IAEA Safeguards Agreement, and other accords. The International Physical Protection Advisory Service (IPPAS), an IAEA program dedicated to helping member states strengthen their physical protection programs, has evaluated Russia's nuclear security approaches and made recommendations. The IAEA, then, has provided some useful services. This international involvement provides a channel for Western standards, values, and management practices to influence Russia's nuclear sector, including its security culture. Bilateral MPC&A cooperation with and assistance from the United States and European countries is a substantial source of innovative ideas and approaches.

Another agency with responsibility for nuclear safety and security is Rostekhnadzor, the successor to the reformed Gosatomnadzor. Created in the wake of the sweeping 2004 administrative reform, Rostekhnadzor retained all functions and responsibilities relating to nuclear safety and security oversight. It can initiate legislation and normative acts, and it establishes industry-wide norms and procedures for ensuring material safety and security. Licensing nuclear facilities and monitoring material protection, control, and accounting (MPC&A) arrangements are some of the functions performed by Rostekhnadzor.[4]

Rostekhnadzor is also closely involved in a number of international cooperative projects intended to help modernize and improve Russia's national system of nuclear MPC&A. Specifically, Rostekhnadzor works with the EU Commission, the IAEA, and the European Bank for Reconstruction and Development on a number of projects in Russia.[5]

There is a certain disconnect between Russia's proactive support for nuclear security internationally and its reluctance to acknowledge the vulnerabilities and weaknesses of its own nuclear sites. On the one hand, Russian officials are quite emphatic in acknowledging, as Rosatom

4. "Provisions for the Federal Service for Ecological, Technical, and Atomic Oversight," Government Resolution no. 401, July 30, 2004, <http://government.ru/institutions/ministries/docs.html?he_id=1024>.

5. "Cooperation with International Organizations Section," Rostekhnadzor Website, <http://www.gan.ru/mezh_s/mezh_s1.htm>.

Director Alexander Rumyantsev explicitly did at the IAEA General Conference in September 2004, that "the available evidence of diversion of nuclear and radioactive material in a number of countries makes it imperative for governments and international organizations to strengthen nuclear security."[6] On the other, they resist admitting that Russia itself belongs to this category of countries and that, partly for reasons beyond its control, it can be easily characterized as a weak link in global nuclear security. For example, despite indisputable evidence to the contrary, Rumyantsev has adamantly maintained that, over the past 25 years, as little as 100kg of non-weapons-grade natural uranium was stolen in Russia. He further insisted that the quantity of weapons-grade uranium stolen was measured in tens of grams, and that it had all been located and retrieved.[7] A major problem, in view of a U.S. nuclear expert, is a "lack of acceptance" within the Russian government that "their materials are not adequately secured and that there is a relationship between terrorism and these materials."[8] This penchant for hedging, then, stems both from Russia's unwillingness to publicly air its dirty linen and from its political ambition to project itself as a leading player in nuclear nonproliferation.

The term "nuclear security culture" is rarely used in official Russian directives. However, some of these directives incorporate certain properties of security culture and state that these are essential ingredients of security and physical protection. The December 2003 document enunciating "Principles of State Policy for Nuclear Security and Radiation Safety," for example, identifies four priorities that will improve physical protection:

- a more comprehensive legal basis
- threat and vulnerability assessment
- evaluation of physical protection
- information protection

Of note, the document does not specifically pay tribute to the cultural dimension of security. Instead of security culture, regulatory documents in the nuclear industry typically speak of the "human factor," i.e. professionalism and competence, as a critical element of the overall security architecture. In this context, breaches of security are attributed to oversight, professional mistakes, and malicious intent. These documents recommend a methodology to deal with such problems, but it falls short of the comprehensive strategy needed to realize a multifaceted and vibrant nuclear security culture.[9]

Despite the lack of official recognition or practical guidance regarding security culture, some Russian experts have elaborated their own vision and understanding of this concept. In one instance they defined security culture as an integration of values, technical concepts, moral norms, and behaviors manifested at three tiers: policymaking, management, and individual behavior. An important characteristic of most Russian approaches is that they tend to merge and intertwine safety and security much more closely than does the methodology suggested in Chapter I, which derives

6. "A Major Dimension of Combating Nuclear Terrorism," *RIA Novosti*, September 19, 2004.

7. "Over 25 Years 100 kg of Natural Uranium Has Been Stolen in Russia," Newsru.com, September 16, 2004, <http://newsru.com/russia>.

8. Interview with Laura Holgate, vice president of the Nuclear Threat Initiative, in "U.S. Expert Sketches Nightmare Nuclear Terrorist Attack on Major City," September 22, 2004, <http://www.spacewar.com>.

9. Office of the President, "The Principles of State Policy for Nuclear Security and Radiation Safety and Security in the Russian Federation for the Period Through 2010 and Beyond," Presidential Directive no. PR-2196, December 4, 2003, <http://www.scrf.gov.ru/Documents/Decree/2003/2196.html>. The document specifies measures for improving security by 2010. However, none of these measures amounts to an innovative personnel management policy able to transform the culture of an organization.

from prevailing Western practices. One possible reason for the disparity between our approach and theirs is that Russians have treated safety as a far higher priority than security since the 1986 Chernobyl incident. They view security as a lesser concern, moreover, because they believe that breaches of security typically lead to safety problems. Linguistics also plays a role: While English makes a clear distinction between safety and security, the two terms are often translated into Russian as the same word, *bezopasnost.*[10]

Despite some ambivalence on the part of Russians, the program on nuclear security culture administered by the U.S. Department of Energy (DOE) continues to win new converts in the Russian nuclear sector. Rosatom professional training institutes are now poised to offer relevant training programs to top- and mid-level site managers. With the help of DOE funding, Russia's nuclear sector has introduced security culture coordinators at several sites on an experimental basis. If this project succeeds despite numerous political and organizational hurdles, considerable strides will have been made toward achieving high standards of nuclear security culture in Russia.

Although it shares responsibility for the security of nuclear materials with other executive agencies, Rosatom is responsible for taking inventory of all government-owned nuclear materials. Other agencies possessing nuclear materials include the Russian Academy of Sciences, the Ministry of Education and Science, the Ministry of Transportation, the Ministry of Industry and Energy, and the Kurchatov Institute. In addition, there are numerous users of radioactive sources in the health, agricultural, food processing, space, aviation, geological, customs, construction, and chemical sectors. Given the threat of terrorism featuring nuclear weapons or "dirty bombs," any methodology designed to implant security culture must eventually go beyond Rosatom and be adjusted to other urgent needs. For this evolution to happen, industry leaders must understand that security culture is part of the overall professional culture. Improving it can pay dividends not only for security, but also for better safety, higher productivity, and more efficient management. Persuading industry that it can serve its own interests while bolstering security culture will be one of the chief tasks of any training regimen.

4.2 Facility Leadership

4.2.1. Top Management

Top-tier managers at Russian facilities, meaning directors, first deputy directors, and chief engineers,[11] are likely to view improving site security as an important function. For them this is a personal matter: Facility directors are personally liable for breaches of nuclear security and are required under the Law "On the Use of Atomic Energy" to establish adequate physical protection systems. Lapses in security could result in facilities shut down and licenses revoked–with the accompanying adverse impact on revenues, competitiveness, reputations, and careers. Leaders wield substantial influence over the assumptions and ideas within an organization because they decide what the organization will do, what it will not do, and what standards it will adopt. They can use their positions of power

10. Authors' interviews with Irina Kupriyanova, Institute of Physics and Power Engineering, and Vladimir Kornelyuk and Konstantin Dushutin, Moscow Institute of Professional Training, September 25, 2003 and February 18, 2004.

11. The *Chief Engineer* defines and implements technical policy and assures the safe and secure operation of the facility. Also, the chief engineer manages and controls programs related to safety and security. In addition to being in charge of providing regular support of electric energy and thermal energy, the chief engineer organizes technical control of design, accounting, and certification of workplaces at the facility, personnel training and retraining, and job description formulation. Moreover, the chief engineer organizes research and studies at nuclear facilities, manages the use of nuclear energy, and assimilates international experience. The position is responsible for preventive maintenance, accounting, the safe storage, use, and transportation of nuclear materials, spent fuel, and wastes, and coordination between contractors and facility deputies. "Job Descriptions of Top and Mid-Level Managers Responsible for MPC&A," *Ministry of Labor and Social Development Bulletin* 5 (May 2001).

to intervene at all levels of the organizational hierarchy, reshaping the workplace culture. They can encourage new and different assumptions and patterns of thinking among their colleagues, establish new patterns of behavior, and change the physical environment, language, and guiding principles associated with the organization. This is no less true for nuclear security culture.

In addition to developing physical protection systems and assessing the effectiveness of these systems, Russia's top nuclear managers are tasked with:

- conducting vulnerability assessments
- assessing economic and environmental damage
- developing normative acts and plans
- supervising the implementation of relevant instructions[12]

Whether a given facility can achieve a high standard of security culture depends to a great extent on the commitment and dedication of top managers. They are doomed to fail in this task unless they themselves have a deep-seated belief that there is a real and present threat. To this end, Russia's normative documents are explicit about existing threats to nuclear material and facilities. If adequately substantiated and clarified to top managers, the claims made in these documents would provide powerful assumptions on which to found a more efficacious security culture. A partial list of threats includes:

- diversion of nuclear material and its products, as well as unauthorized access to information about nuclear material and technologies
- acts of terrorism or sabotage at nuclear sites or storage facilities
- nuclear blackmail[13]

Potential sources of these threats include:

- premeditated actions of terrorists or the agents of governments intent on obtaining nuclear know-how, possibly abetted by insiders who in some circumstances may act on their own
- mistakes and incorrect actions by operating personnel
- equipment failure
- natural disasters[14]

One important challenge for senior managers is to discard the old approach to physical protection, which was premised solely on defeating external threats. Insider threats commanded

12. Authors' interview with Konstantin Dushutin and Vladimir Kornelyuk, Moscow Institute of Professional Training, December 23, 2003.

13. "Concept of Federal System for Nuclear Materials Control and Accounting," Government Resolution no. 1205, October 14, 1996; Federal Program, "Nuclear and Radiation Safety and Security in Russia for 2000-2006"; "Main Rules for Nuclear Materials Control and Accounting," Government Resolution no. 746, July 10, 1998; "Main Rules for Nuclear Materials Protection," Government Resolution no. 264, March 7, 1997; Office of the President, "Principles of State Policy for Nuclear Security and Radiation Safety and Security."

14. Authors' interview with Konstantin Dushutin and Vladimir Kornelyuk, Moscow Institute of Professional Training, December 23, 2003.

little attention. This approach is at variance with new realities. Russia's regulatory documents direct facilities to readjust their outlook to these new realities. However, this has proved painful for many organizations, largely because of aging nuclear workers who are resistant to change, a lingering reluctance to report on one's colleagues, and other factors. Over the long term, Russia's current reliance on the human factor to guarantee security is supposed to give way to more technology and automation. According to some sources, the evolving approach of the Russian government towards security is based on the assumption that the reliability of human-based security systems is about 50 percent, compared to about 90 percent for automated security systems.[15] A fully automated system is still a long-term objective for Russia, however, and, even after it is put in place, its operation and maintenance will continue to depend on human input.

Only by setting high standards for themselves can Russian senior managers promote the spirit and the guiding principles that lead to an effective nuclear security culture. However, this is not a task that can be accomplished in isolation from other management tools. An effective security culture cannot exist without a good overall management system, which supplies (as seen in Chapter I) the performance standards, procedures, inspections, and myriad other instruments that form the groundwork for a thriving nuclear security culture.

Accordingly, a major step towards improving nuclear security culture is for top managers to acquire the managerial skills to run their facilities more efficiently and smoothly. Rosatom has been developing a set of criteria for recruiting nuclear industry leaders. The recruitment and management system as it exists in Russia makes it very difficult, however, to fire managers for substandard performance. Entrenched interests will persist until it becomes easier to dismiss subpar managers. There are five such basic qualifications for top directorship positions:

- personal qualities (responsibility, compliance, persistence, etc.)
- organizational skills (rational use of resources, ability to form partnerships with others, ability to motivate personnel, etc.)
- professional competence (educational background in a relevant discipline, demonstrated understanding of free-market mechanisms, knowledge of nuclear-related laws and regulations, etc.)
- psychological status (leadership qualities, emotional stability, self-control, capacity to respond to threats and emergencies, etc.)
- social standing (personal commitment to security culture, solid principles, ability to lead by personal example, etc.)[16]

By law, directors of Russia's nuclear facilities must be recertified every five years in order to have their contracts extended. The curriculum for recertification training sessions includes a nuclear security module and a paper. Many prerequisites for instilling nuclear security culture among top managers are now in place, but how aggressively managers pursue these goals at their facilities depends on the attitudes, policies, and funding priorities handed down by the national and industry leadership.

---

15. Authors' interview with Yuri Volodin, head of department at Rostekhnadzor, September 17, 2004.

16. Authors' interview with Konstantin Dushutin and Vladimir Kornelyuk, Moscow Institute of Professional Training, December 23, 2003.

4.2.2 Mid-level Management

Mid-level managers are assigned hands-on responsibility for security policy. The makeup of this group varies from facility to facility, usually including deputy directors for safety and reliability,[17] deputy directors for MC&A,[18] and deputy directors for physical protection.[19] At smaller organizations these functions are performed by heads of combined departments of physical protection and accounting and control.[20] Department heads implement industry and site security guidance, manage and oversee operators and other lower-level personnel, and have direct access to nuclear materials. They are the chief purveyors of nuclear security culture.

Mid-level managers put into practice security concepts and policies approved by their superiors. Under Rosatom's official definition of their functions, the middle tier of management is responsible for:

- supervising the implementation of security-related work
- developing job descriptions for all categories of security personnel
- organizing periodic updates to the relevant instructions
- administering rewards and punishments to motivate personnel
- launching periodic reviews of work projects
- organizing training sessions designed to improve security awareness and job skills
- compiling written instructions to acquaint employees with their duties[21]

---

17. The *Deputy Director for Safety and Reliability* ensures nuclear and radiological safety, monitors the safety of operations and the reliability of equipment, and organizes preventive maintenance. He organizes the accounting and analysis of equipment malfunctions in order to improve reliability. In case of an accident, he supervises post-accident evaluation. He promulgates safety-related information among the workforce and participates in the certification of working positions. "Job Descriptions of Top and Mid-Level Managers Responsible for MPC&A," *Ministry of Labor and Social Development Bulletin* 5 (May 2001).

18. The *Deputy Director for Material Control and Accounting* ensures control and accounting of nuclear materials, as well as the overall security of nuclear and radioactive materials at the facility. He enforces compliance with safety and security rules, controls access to sensitive areas, provides reports on state-of-the-art nuclear materials at the facility, participates in the initial evaluation of accidents and their scope, cooperates and interacts with the deputy director on material protection, and tests personnel on their knowledge of material control and accounting. "Job Descriptions of Top and Mid-Level Managers Responsible for MPC&A," *Ministry of Labor and Social Development Bulletin* 5 (May 2001).

19. The *Deputy Director for Physical Protection* ensures physical protection and oversees the installation and use of security hardware, supervises efforts to prevent nuclear-materials smuggling, ensures that nuclear materials are securely stored, investigates cases of smuggling and leads efforts to recover smuggled materials, and provides vulnerability analysis to help improve the physical protection system. He establishes measures to assure the security of state and commercial secrets, represents the facility in the Security Service and Internal Affairs Ministry, participates in inspections together with GAN, and helps the Federal Security Service and Ministry of Internal Affairs implement preventive measures related to the security of nuclear materials. He also organizes the evacuation and treatment of personnel when emergencies occur. He hires personnel for the department of physical protection. "Job Descriptions of Top and Mid-Level Managers Responsible for MPC&A," *Ministry of Labor and Social Development Bulletin* 5 (May 2001).

20. The *Department Head for Physical Protection* is responsible for material protection at the facility. He oversees technical and organizational measures that safeguard the security of nuclear materials, manages the MPC&A system as a whole, and acquires information necessary to ensure the physical protection of nuclear materials and the preservation of secrets. He also conducts inspections and informs top management about violations, disclosure of state secrets, or other unsanctioned actions involving nuclear materials. Finally, he ensures personnel training and retraining in nuclear security. The *Department Head of Nuclear Materials A&C* is responsible for accounting and control and inventory of nuclear materials, as well as personnel training. He participates in the certification of working places, and is expected to know the laws and regulations pertaining to the development of atomic energy, as well as the documents related to MC&A and inventory, nuclear security and safety, design and operation, and personnel protection. "Job Descriptions of Top and Mid-Level Managers Responsible for MPC&A," *Ministry of Labor and Social Development Bulletin* 5 (May 2001).

21. Authors' interview with Konstantin Dushutin and Vladimir Kornelyuk, Moscow Institute of Professional Training, December 23, 2003.

Negligent mid-level managers can ignore security measures, bypass or disable security devices, or force personnel to ignore security procedures. Indeed, they have the knowledge, skills, and authority to arrange diversions of material from the facility if so inclined. Not surprisingly, then, most diversion cases have involved collusion by mid-level management. The diversion of material from the Elektrostal facility in 2000 and the 2003 theft of uranium by the deputy director of a firm that maintains Russian nuclear icebreakers stand out as examples of the malfeasance that can take place.[22] If top managers are pivotal in launching a security culture campaign, mid-level managers are important in supervising and sustaining it on a daily basis.

4.2.3 Rising Nuclear Managers

Most high- and mid-level nuclear managers in Russia are expected to retire within the next five to ten years. Few professionals were recruited into the industry during the tumultuous 1990s, breaking a tradition under which children succeeded their parents when the parents retired. Consequently, the young generation now entering the field will vault into positions of senior leadership with unprecedented speed–opening possibilities for rapid cultural transformation.

In July 1997 the Russian president issued a decree "On Training of the Future Leaders for the National Economy," better known as the "Presidential Program." Some prior managerial experience was required of applicants for the Presidential Program. According to program guidelines, 5,000 young managers under the age of 40 were to be trained for various sectors within five years. Of that total, 500 were designated to work at Minatom. Facility and industry leaders chose prospective managers through stiff competition. Minatom requested and received the authority to train its own young leaders. The Moscow Institute for Professional Training, together with the Moscow State Institute for Physics and Engineering, won the tender. The Presidential Program was extended beyond 2002.

The youthful elite is the most vocal and proactive component of Russia's nuclear sector. Their orientation is more practical and businesslike. They are more likely than their older peers to accept, understand, and promote technical innovations in the security arena. Exposing them to security culture and new ways of thinking helps mitigate the reflexive suspicions to which the elder generation is prone, and they are more open to new ideas.[23] Winning them over to nuclear security culture is a long-term investment which will pay off as young managers ascend the hierarchy of the nuclear sector.

Russia's nuclear sector has been treating security threats quite seriously, but is acutely sensitive to negative publicity and thus has been slow to make its operations more transparent. At the same time, it still lacks an integrating strategy, clear job descriptions, and worthy role models at the facility level. Nuclear security culture can fill in these gaps and contribute to better standards of physical protection. As an integral part of the overall professional culture, security culture can provide substantial benefits to an organization beyond security. Collateral improvements to safety, productivity, and general management can translate into greater acceptance of the new concept by reluctant managers. ■

22. Anna Badkhen and James Sterngold, "Nuclear Theft Case Raises Fears about Russia," *San Francisco Chronicle*, November 23, 2003.

23. Michael McFaul, *Generation Change in Russia*, CSIS Working Paper Series no. 21 (Washington, DC: Center for Strategic and International Studies, 2002). For more information on generational change, see also William Dudley, ed., *Russia: Opposing Viewpoints* (San Diego, CA: Greenhaven Press, 2001); Timothy J. Colton and Robert Legvold, eds., *After the Soviet Union: From Empire to Nations* (New York: W. W. Norton & Company, 1992).

CHAPTER V

PERSONNEL PERFORMANCE

In dealing with the issues associated with Russia's nuclear personnel and security culture, it is imperative to understand the challenging environment in which these people operate. On the one hand, nuclear personnel have to improvise and use extraordinary discretion in order to fill the gaps in the nation's still-incomplete legal and regulatory framework. On the other, a wide range of emergency situations, from terrorist attack to unexpected power outages, makes it necessary to instill in them discipline and the habit of strict compliance with rules. As a result, improving personnel performance in the Russian nuclear sector demands a careful blending of what may be regarded as routine Western standards with conditions unique to Russia.

Another major observable problem at nuclear facilities in Russia is that, even with modern security hardware in place, personnel frequently misuse and mismanage their equipment. A U.S. General Accounting Office (GAO) report in February 2001 cited several cases in which equipment had been used improperly.[1] Gates were left open and unattended. Guards routinely failed to respond to alarms or check the identification of personnel entering sensitive areas that housed nuclear material. In many cases equipment was left uninstalled or inoperable. Indeed, mid-level managers sometimes bypassed or disabled security equipment. At several facilities, security procedures were violated systematically: Either the personnel assigned there failed to understand the procedures correctly, or procedures simply were not in place.[2] One report from the National Intelligence Council to the U.S. Congress mentioned that guards sometimes abandoned their posts, and at one location an alarm system worked only half the time.[3] These patterns of behavior point to a seriously flawed security culture.

Security was not much of a problem in the Soviet Union. The Soviet nuclear security system was based on the so-called 3G model–guns, guards, and gates–which prioritized armed guards and was reinforced by the Communist ideology, totalitarian controls, a rigorous system of security clearances, and the country's political isolation from the rest of the world. This unique environment made the 3G model work during the Soviet period. Moreover, the prestige of working in the nuclear industry, which was deemed to be the key to national survival in the standoff with the United States, discouraged bad or negligent behavior. Moral satisfaction, pride, and material incentives such as high wages and benefits also contributed to the efficacy of this low-tech security system.

---

1. According to one report by the U.S. General Accounting Office, *Security of Russia's Nuclear Materials*, GAO-01-312 (Washington, DC: Government Publishing Office, 2001), p. 12, at three out of nine sites visited by the GAO, "some problems appeared to decrease the effectiveness of the new systems. For example, one site left a gate to its central facility opened and unattended during the day. According to a site official, the gate was left open to allow employees to enter and leave the facility without having to use the combination locks on the gate. When the gate is open, the only other controlled access point is on the perimeter of the site. At another site the guards did not respond to metal detectors that were set off when the GAO team entered the site, nuclear materials portal monitors were not working, and the alarm system had exposed cabling that could allow an adversary to cut the cable and disable the alarm easily. At the third site, the DOE had provided heavy metal containers that could be bolted to the floor to make it more difficult for an individual to gain access to the material, but some of the containers were empty, and the site stored material in old containers that did not offer as much protection. In addition this site did not have access controls, such as material detectors or nuclear material portal monitors at locations where nuclear material is stored, and the guards did not check the identification of the people entering the storage areas."

2. Irina Koupriyanova, "Assessment of Effectiveness of U.S. MPC&A Assistance to Russia," *Yaderny Kontrol* 2 (March-April 2002): pp. 57-65.

3. U.S. National Intelligence Council, *Annual Report to Congress on the Safety and Security of Russian Nuclear Facilities and Military Forces*, February 22, 2002, <http://www.cia.gov/nic/pubs/other_products/icarussiansecurity.htm>.

The collapse of the Soviet Union, however, changed most of these factors or rendered them irrelevant almost overnight. With the opening of borders, the shift to a free-market economy, and the lack of a new ideology to replace Communism, Russia and its nuclear sector have undergone a difficult period of transition toward new standards of personnel performance and professional culture.

5.1 Professional and Work Culture

Work culture is understood to be "a pattern of basic group assumptions that has worked well enough to be considered valid, and, therefore, is taught to new members as the correct way to perceive, think and feel."[4] A desirable work culture includes shared institutional values and priorities, rewards and other practices which foster inclusion, and a commitment to performance, while still allowing for diversity in thought and action. Russia's evolving professional culture is currently a combination of the Soviet and Western approaches.

5.1.1 Impact of History and Tradition

Cultures are neither good nor bad in themselves; they are good or bad at shaping certain values in accordance with the perspectives and priorities of the larger society or institution. Thus a particular organization can have a culture that is good at achieving one type of result, but poor at achieving another. That is why nuclear security culture needs to be examined specifically. It cannot be assumed to exist just because the organization's performance is otherwise healthy or not to exist just because performance is otherwise unhealthy.[5] By way of illustration, below are specific examples showing how history and tradition bear on Russia's standards of professional culture in general and security culture in particular:

- *Russian Orthodox and Communist ideologies.*[6] As opposed to the individualism of Western ethics, Orthodox values, combined with the tsarist past and the Communist ideology, have contributed to a deemphasis on personal responsibility and a strong emphasis on collectivism. Suppression of individualism and promotion of collectivist values have engendered a mentality that predisposes Russians to wait passively for commands from above and to shun personal responsibility. Russians typically do not risk challenging the leadership and its authority. The prevailing antipathy toward personal responsibility poses a serious impediment to an effective security culture.
- *"Special path."*[7] Many Russians see their country as following a "special path" blending Western and Eastern cultures.[8] To them Russia is fundamentally different from other countries and nations. It has a special mission to perform. This messianic perception is reinforced by the still-

4. Edgar H. Schein, *Organizational Culture and Leadership: A Dynamic View*, 3d ed. (San Francisco, CA: Jossey-Bass), p. 47.

5. For more information, see R. H. Kilmann, M. J. Saxton, and R. Serpa, "Issues in Understanding and Changing Culture," *California Management Review* 28 (1986): pp. 87-94.

6. For example, see, Nuclear Disarmament Forum, *Sustainable Disarmament* (Switzerland, 2002); Rosemary H. T. O'Kane, *Paths to Democracy: Revolution and Totalitarianism* (London: Routledge, 2004).

7. For example, see S. Kara-Murza, *Soviet Civilization* (Moscow, 2002); Yitzhak Brudny, Jonathan Frankel, and Stefani Hoffman, eds., *Reconstructing Post-Communist Russia* (Cambridge: Cambridge University Press, 2004); James H. Billington, *Russia in Search of Itself* (Washington, DC: Woodrow Wilson Center, 2004); Nikolas K. Gvosdev, ed., *Russia in the National Interest* (New Brunswick, NJ: Transactions Publishers, 2004).

8. Thomas Graham, *Russia's Decline and Uncertain Recovery* (Washington, DC: Carnegie Endowment for International Peace, 2002).

prevalent view of Russia as a politically, culturally, and otherwise unique superpower. This sense of exceptionalism constrains the willingness of Russians to accept U.S. and international help in such sensitive areas as security. U.S. personnel working with Russian partners often mention a gulf between their security culture and risk perceptions and those of Russians. According to a specialist from the National Aeronautics and Space Administration, Russians are comfortable with risk. They consider themselves less rigid and more intense than Americans, who tend to follow their technical manuals to the letter, and thus more flexible in approaching technical problems. While in the United States the key principle is "prove it is safe," in Russia it is the opposite. The different approaches contribute to communication problems.[9]

- *Human-based versus machine-based command.* A recent chain of industrial accidents and disasters is partly explicable as a long-predicted failure of decrepit Russian equipment and obsolete technology. It is also a reminder of the importance of the human factor to all types of human endeavor, including the nuclear sector, where safety and security must be at the forefront of the organization's activities. Although the importance of the human factor in such matters is not unique to Russia, it is much more pronounced there because of the differences in how Russians and Westerners think about the application of technology and the role of personnel.[10]

  A tragic air collision that took place on July 2, 2002 exemplifies the contrast in cultural mentalities. A Russian passenger jet carrying dozens of schoolchildren struck a DHL cargo plane over Germany. The Russian and Western aircrews responded to the emergency far differently. Western procedures require pilots to rely exclusively on the data and information provided by the onboard computer and other equipment, and to treat warnings and instructions from the air-traffic control tower as recommendations. In stark contrast, Russian regulations give priority to verbal instructions from the ground. These instructions override the information from devices in the cockpit.

  The accident demonstrates that cultural differences reflected in policy and procedures could have disastrous consequences in the nuclear sector–especially if Russian and foreign entities trying to cooperate on matters related to material protection, control, and accounting (MPC&A) saw the issues differently.

- *Flawed incentive structure.*[11] In the Soviet epoch stark inconsistencies between the proclaimed goal of achieving Communism and the reality of shortages of basic consumer goods, corruption, and political protectionism generated cynicism and political apathy.[12] Far from commanding the loyalty of Soviet citizens, the system became something to be beaten. The rift between ideals and reality prevented the formation of a norm-abiding mentality. Indeed, people tried to avoid the norms rather than abide by what they viewed as a morally bankrupt system. Low productivity among this apathetic workforce only compounded the problem. Rewards in the form of salary, career development, and so forth were never tied to performance. As late as 2003, the vast majority of respondents in one public-opinion poll–81 percent–did not consider diligence to be a key prerequisite for highly paid careers. Rather, they attributed success to favorable circumstances, a good relationship with management, or simple luck.[13] Nuclear industry

---

9. "U.S., Russian Cultures Clash in Orbit," CNN.com, November 11, 2003.

10. For example, see A. Korolev, A. Roumyantsev, B. Sishkin, and A. Shmarin, "The Probabilistic Analysis of Effectiveness of the MPC&A Upgrades," Paper Presented at an MPC&A International Conference in Obninsk, Russia, May 22-26, 2000.

11. For example, see *Russian Transformations: Challenging the Global Narrative*, ed. Leo McCann (London: Routledge Curzon, 2004); William Dudley, ed., *Russia: Opposing Viewpoints* (San Diego, CA: Greenhaven Press, 2001); Ajay Goyal, "Russia's Untapped Treasures," *Russian Journal*, <http://www.norasco.com/ ajay_goyal_6.html>.

12. For example A. Kuznetsov and N. Zakharov, "Specifics of Job Motivation in Russia," <www.znl.boom.ru.kuz.htm>.

managers lament that, with the disappearance of the Soviet-style enforcement of discipline, they have to deal, often unsuccessfully, with the legacy of the double-standards syndrome. Lax discipline makes it impossible to enforce security regulations and arrangements.

- *"Scapegoat" mindset.*[14] During the Soviet era, glaring societal and economic inconsistencies could not be officially attributed to any flaws in the political system. Consequently, these intrinsic shortcomings in the system were systematically ignored or explained away as sabotage by "enemies of the people," the product of foreign conspiracies, or mistakes by specific individuals. The performance of the Communist Party or the political system was never called into question. Specific failures were officially investigated, those found guilty were punished, and the problem was considered resolved until the next incident. This practice instilled a scapegoat mentality that reflexively blamed individual error or ineptitude, instead of looking for causes within the system.

  This mentality persists in the nuclear industry, where management does not always deal with errors by trying to find their causes and fix them, but rather seeks to place the blame on a specific individual. Unlike the U.S. Department of Energy (DOE), Russia's Federal Atomic Energy Agency (Rosatom) has not yet established a comprehensive database for identifying systemic causes of industry-wide incidents that involve security. Since the root causes of security breaches are not always found and fixed, errors and problems can be repeated. Also, the scapegoat mindset impedes efforts to cultivate an attitude of questioning and reporting among facility staffs.

- *Lack of transparency.*[15] The Soviet political system was based on excessive secrecy, compounded by a widespread mania about Western espionage. The nuclear sector in particular excelled at imposing secrecy. The secret services (the NKVD, MGB, and KGB) and their director throughout the 1940s and early 1950s, Lavrentiy Beria, were directly responsible to Joseph Stalin for building and tightly controlling the nuclear defense industry. Security officials monitored the production of fissile materials and the development of nuclear weapons by being physically present at each and every stage of the process.[16]

  The Soviet apparatus, then, imposed an impenetrable veil of secrecy whose remnants are effectively enforced, even in the post-Communist period. The Federal Security Service (FSB), one of several successors to the KGB in today's Russia, has a mandate under federal law to ensure the security of nuclear facilities, among other things.[17] FSB officers are routinely assigned to perform a variety of security-related functions such as screening job applications, investigating security breaches and taking preventive action, and helping develop internal regulations for physical protection.

---

13. Public Opinion Foundation, Public Opinion Poll, September 11, 2003, <http://www.fom.ru>.

14. For example, see Anders Åslund and Martha Brill Olcott, *Russia after Communism* (Washington, DC: Carnegie Endowment for International Peace, 1999); V. Yadov, ed., *Russia: A Transforming Society* (Moscow: Institute of Sociology of the Russian Academy of Science, 2001). See also studies by the Russian Institute of Sociology and the Institute's publications *SOCIS* and *SOCIO-LOGOS*, <http://www.isras.ru/?page=journals&sub=logos>.

15. For example, see Sarov Analytical Nonproliferation Center and Institute of Strategic Stability, *Nuclear Disarmament, Nonproliferation and National Security*, 2001, <http://www.iss.niiit.ru/book-2/index.htm>.

16. Nina Khrushcheva, the granddaughter of former Soviet leader Nikita Khrushchev, examined Russia's "culture of contempt." As she put it, this culture is based on fear and jealousy. Khrushcheva claims that Russians view regulations and rules not as instruments written to make their life easier but as instruments of control. According to her, Russia tries to superficially imitate Western culture, but not to accept it. Lack of transparency and limited access to information have been one of those instruments of control. Nina Khrushcheva, "Russia's Culture of Contempt," *Korea Herald*, August 5, 2004.

17. "On the Federal Security Service," Federal Law no. 960, August 11, 2004.

This dual responsibility over security-related tasks, coupled with the general lack of transparency in the nuclear sector, tends to erode rather than boost personnel morale. It unnecessarily restricts their participation in security affairs, sets technicians at odds with the security force, and prevents site personnel from being fully integrated into site-wide efforts to improve security standards. This poses an obstacle to the development of a nuclear security culture.

- *Anti-American sentiments.* Many Russians continue to view the United States as an unfriendly nation, thinking in the us-versus-them terms common during the Cold War. Public opinion polls taken since 2002 have consistently shown that about half of the population holds a negative view of the United States and its role in the world.[18] The war in Iraq in 2003 and Russia's refusal to support it only amplified these sentiments. The resulting suspicions further complicate the implementation of U.S.-sponsored nuclear assistance programs in Russia. Although the younger generation on average views the United States more favorably than do the generations reared during the Cold War, the predominance of the older generation among the leadership of the nuclear industry throws up an additional barrier to bilateral cooperation.

5.1.2 Professional and Work Culture in Rosatom

Russia's Ministry of Atomic Energy (Minatom), one of the most prestigious and well-funded government agencies during the Soviet period, had a well-established professional culture and work ethic. When it came to education in nuclear physics and engineering in the USSR, meritocratic principles prevailed over the regime's otherwise egalitarian dogma. A massive search for and careful selection of candidates, an exceptionally qualified teaching staff, and other trappings of elite training were quietly launched and promoted. The Soviet educational bureaucracy considered the recruitment of academically gifted Russians into the field of physics incompatible with long-established guidelines and tried to resist. Stalin's personal involvement in and emphasis on the nuclear sector, however, won out over entrenched bureaucratic interests.[19]

Minatom officials worked assiduously to promote this corporate spirit and culture. Even so, the nuclear sector was not immune from the syndromes and upheavals discussed previously. Working in the Soviet nuclear industry was largely a hereditary affair, with work culture passed down from one generation to the next as children took over jobs from their parents. This made for professional continuity for families living in the closed cities. Recruitment was severely restricted due to the secrecy surrounding the nuclear sector, insider competition for the generous benefits available within the industry, and outsiders' lack of access to closed cities. This all came to a halt after the collapse of the Soviet Union, when the brightest graduates in technical disciplines began to embrace careers in business, law, and computer engineering instead of the nuclear industry. As a result, in the post-Communist period the nuclear sector has experienced an influx of people originally labeled outsiders. These outsiders brought with them new values and their own elements of culture.

Efforts are underway again to promote high standards of performance in the nuclear sector. In 2002, for example, Minatom launched a competition among facilities under its jurisdiction for the title of the "Enterprise with High Standards of Production and Labor Organization Culture."

---

18. Public Opinion Foundation, Public Opinion Poll, September 5, 2003, <http://www.fom.ru>. For more information, see U.S. and Russian Working Groups, *U.S.-Russian Relations at the Turn of the Century* (Washington, DC: Carnegie Endowment for International Peace, 2000).

19. Igor Khripunov and Maria Katsva, "Russia's Nuclear Industry: The Next Generation," *Bulletin of the Atomic Scientists* 51 (March/April 2002): p. 52.

Working jointly with union leaders, Minatom developed a list of 17 criteria according to which the candidates for the prize would be judged. The personnel of the winning facility would divide $100,000 worth of bonuses among themselves annually.[20] The winner for 2003 was the Novosibirsk Chemical Concentrates Plant. Unfortunately, none of the 17 criteria involved promoting security. If the rules were adjusted to correct this shortcoming, the Rosatom contest could provide a vehicle for elevating security culture standards.

One major problem in the Russian nuclear industry today is the shortage of middle managers. Many managers washed out of the industry after the breakup of the Soviet Union, creating a void in the managerial hierarchy that originally weakened efforts to rebuild security within the nuclear sector. Since the late 1990s, however, the nuclear industry has become more attractive to young people. The influx of younger leaders who readily accept high-tech approaches to security will facilitate the introduction of a healthier attitude toward security, provided these young leaders are adequately trained and motivated. A better security culture should materialize in the coming years as young people move up to fill posts in middle management.

5.2 The Importance of Motivation

Human errors account for more than half of mishaps in the nuclear industry. In 2000, a nongovernmental organization, the Prognoz (Forecast) Center, conducted a survey among employees of Russian nuclear power plants. The survey found that about half of all personnel errors were due to "carelessness," which was defined broadly to include a lack of training, an inadequate understanding of the importance of complying with rules and regulations, or the consequences of being inattentive; 20 percent of violators did not know the instructions and regulations; and about 30 percent of violators knew the rules but did not want to follow them. Except for violations caused by a lack of skills and training, the bulk of personnel errors–with carelessness and deliberate violations of norms totaling some 70 percent–accrue from a lack of motivation in the workforce.[21]

As mentioned previously, during the Soviet era, working in the nuclear industry brought prestige and high salaries and benefits. The collapse of the Soviet Union negated these incentives. Many nuclear facility personnel took second jobs in order to survive and support their families, and they explored a wide variety of alternative sources of income. Security was far from the top concern for personnel and managers. Security awareness was lacking, and there were few incentives for personnel to follow security procedures. Top management at the sites failed to prioritize security over other tasks. Instead they placed tremendous emphasis on boosting production and improving sales. Low salaries and widespread corruption made them vulnerable to bribes and blackmail. Remnants of the Soviet mentality described earlier in this chapter eroded workers' dedication to security. In 1998 a Russian ergonomics laboratory conducted surveys at several Russian nuclear facilities. Fifty-six percent of respondents said that personnel had no real incentive to follow operating instructions, including directives related to security.[22]

If anything, professional motivation is even more important for Russia than it is for Western states, which by-and-large do not suffer from obsolete equipment, incomplete legal frameworks,

---

20. Ministry of Atomic Energy, Minatom Order no. 602, December 19, 2002, <http://www.minatom.ru>.

21. Authors' interview with Vladilena Abramova, Director of Prognoz Center, October 2000.

22. Gennady Zhuravlyov, *From Theory to Practice: Psychological Foundations of Safety Culture in Nuclear Energy and Industry* (Moscow, 1998). For more information, see Gennady Zhuravlyov, *Safety Culture in Nuclear Industry: A Psychological Concept* (Moscow, 2000); Gennady Zhuravlyov, "Safety Culture and Mentality," *Prikladnaya Psikhologiya* 3 (1998); Vladilena Abramova et al., *Psychological Methods of Personnel Management at Russian Nuclear Plants* (Moscow, 1990); Aleksey Anokhin and Vladislav Ostreikovskiy, *Ergonomics of Russian Nuclear Power Industry* (Moscow, 2001).

inadequate training, or poor enforcement practices. Performance incentives used in the West include material inducements, for instance generous salaries, career stability, and good working and living conditions, while personal inducements include recognition, prestige, and personal empowerment.

The United States has enjoyed relative success helping the Russian military improve its security arrangements. Indeed, bilateral projects have been implemented much more smoothly than in the civilian nuclear complex. MPC&A upgrades at naval facilities are still considered to be the chief success story for U.S.-Russian cooperation in this area. Two obvious reasons for this success are the military's discipline and its long tradition of obeying orders. In any event, military personnel are inherently more responsive to specific instructions and seemingly do not need as much external motivation as civilian personnel.

Can the success in the military sector be replicated at civilian sites with the use of different tools? Factors affecting the selection of a motivational approach for a given civilian worker include his or her age, his or her seniority within the workforce, and the location of the facility. At present very few incentives are designed specifically to improve security. Existing incentives are targeted at making nuclear careers more attractive, retaining professionals already working in the nuclear complex, and recruiting young employees and college graduates. However, a carefully tailored package of incentives could have a direct impact on security. At facilities that employ young, motivated professionals and that make security a routine part of their professional training, employees appear more receptive to security culture requirements.

Several motivational tools available to the nuclear sector may directly or indirectly contribute to a better security culture:

- Rosatom has been experimenting with techniques to encourage positive attitudes towards the use of security equipment. Some facilities have begun paying bonuses for maintaining and properly operating such equipment. One example is the Novosibirsk Chemical Concentrates Plant, which instituted bonuses for security equipment operators.[23]

- Broader personnel motivational tools include subsidized mortgages and payment assistance. Several facilities are authorized to issue military service waivers. Others pay college graduates salaries that exceed the facility average. (The latter, however, has an ambiguous effect. While higher salaries help attract young specialists, they also undermine the longstanding seniority- and expertise-based pay system and generate frictions with veteran employees.)

- Retirement benefits are usually insufficient to entice employees to retire and vacate their positions in favor of younger personnel. However, some facilities have introduced efficient voluntary retirement and contract termination schemes. For example, the Siberian Chemical Combine pays employees a lump sum totaling six months' salary if they agree to retire voluntarily.[24] Introducing an early retirement system and additional retirement benefits throughout the industry could speed the advent of a younger generation of nuclear managers with a new professional culture. Diminishing tensions within the workforce through voluntary retirements would also contribute to better security.

23. Authors' interview with a manager at Novosibirsk Chemical Concentrates Plant, Phoenix, AZ, July 13, 2003.

24. Authors' interview with a manager at Siberian Chemical Combine, Phoenix, AZ, July 14, 2003.

5.3 Personal Responsibility

Teamwork is universally regarded as a prerequisite for success. In Russia, however, teamwork often mutates into a form of team dependency that worsens the prevailing lack of personal initiative and responsibility and feeds social infantilism. The Soviet system, characterized by Communist ideology and strong, indeed totalitarian, control, powerfully discouraged personal initiative and responsibility. The system failed to link outcomes with individual performance, thus devaluing individual input and responsibility. This syndrome persists in contemporary Russia. Individual employees may not feel personally responsible for nuclear security, instead assuming that security will, and should, be assured by others. A conviction that personal responsibility lies at the core of security culture is crucial in Russia, where security personnel must be physically and psychologically prepared to combat contingencies ranging from terrorist attacks to power outages, and to react adequately to events that are difficult, if not impossible, to predict.[25]

5.3.1 Inadequate Job Description

Workers' indifference to personal responsibility results in part from poorly defined job descriptions. In May 2001, the Ministry of Labor and Social Development published a manual, *Job Descriptions of Top and Mid-level Managers Responsible for MPC&A at NPP*, that provided job descriptions for facility directors, chief engineers, and deputy directors for physical protection and MPC&A. Although introducing job classifications for people dealing with MPC&A represented a positive step, and while the manual clearly spelled out the responsibilities entrusted to mid-level management, it left the descriptions of top-level positions vague, with duties and responsibilities diffused widely among high-ranking officials. Since different facilities experience different financial conditions–some are profit-makers, others are struggling to survive–many top managers face hard choices as they try to keep their facilities afloat financially while providing adequate resources for security arrangements, as mandated by their job descriptions.

In March 2001, the Center for International Trade and Security at the University of Georgia conducted a survey that asked top-level managers about their priorities and responsibilities. Over 80 percent of respondents did not consider security culture and control of nuclear materials to be their primary responsibility. They maintained that this was "somebody else's responsibility." The survey results were especially worrisome since, as discussed previously, managers who lead by example are the driving force behind the improvement of nuclear security culture.[26]

5.3.2 Whistle-blowing

While the U.S. government has enacted legal protections for whistle-blowers, the Russian mindset frowns upon reporting on one's superiors and colleagues. Whistle-blowing is rarely appreciated. Not only do Russians believe it contravenes the spirit of teamwork, but it is also seen as a throwback to the Stalin era, when informing on one's peers and superiors was encouraged as a means of social and political control. Refusing to report violations and adopting mutually protective cover-up stories when violations are detected is regarded as a sign of loyalty to one's co-workers.

Employees may, however, send complaints to the Russian Professional Union of Employees of Nuclear Energy Industry. The union actively seeks to negotiate improvements to labor conditions and salary policy at nuclear facilities. Employees may also complain to managers about work-related

25. For example, see Timothy J. Colton and Robert Legvold, eds., *After the Soviet Union: From Empire to Nations* (New York: W. W. Norton & Company, 1992); A. Kuznetsov and N. Zakharov, "Specifics of Job Motivation in Russia," <www.znl.boom.ru.kuz.htm>; David C. Thomas, *Readings and Cases in International Management: A Cross-Cultural Perspective* (Thousand Oaks, CA: Sage Publications, 2003).

26. Igor Khripunov, Maria Katsva, and Terrell Austin, "Establishing a Security Culture in Russia: Preliminary Findings," *The Monitor* 7 (spring 2001): pp. 10-14.

issues, including safety and security, but rarely do so for the reasons mentioned above. Sometimes employees send letters of concern regarding environmental safety and security issues to the media, the State Duma, oversight bodies, or other agencies. Of these, the media is considered the most trusted and effective institution and thus is the outlet of first resort.

5.4 Education and Training

Several universities offer degrees allowing graduates to work in the areas of nonproliferation and MPC&A.[27] The Moscow Institute of Physics and Engineering (MEPhI) is the premier educational institute of this kind, offering a graduate degree in MPC&A. As of the end of the 2002-2003 academic year, 40 MEPhI students had earned master's degrees in MPC&A, about 8 per year since the inception of the degree program. However, this program suffers from several problems:

- While MEPhI has been successful in placing its graduates within governmental agencies (Rosatom, Rostekhnadzor, and MPC&A-related organizations such as the Eleron production facility), it has enjoyed less success in placing graduates within nuclear facilities. Facilities generally prefer to employ managers with at least five years of experience and are often willing to train this category of personnel themselves.
- Many of the program graduates do not want to pursue work at nuclear facilities.
- The number of graduates is very small, in large part because MEPhI does not accept applications from graduates of other institutions to participate in its programs.

Rosatom and its forebears have been developing a professional training system since the 1960s. Due to continuing technological progress, new requirements for managers and personnel, and changes in regulatory guidelines, the system was designed to train and improve the professional education of top- and mid-level managers, engineers, and scientists, to establish a "generation succession," and to promote exchanges of information among professionals in the nuclear industry. The programs listed below focus on MPC&A training and have started providing the basics of a nuclear security culture:

- The Russian Methodological Training Center at the Institute for Physics and Power Engineering in Obninsk conducts MC&A training, methodological support, and equipment testing and certification.
- The Interdepartmental Special Training Center at the Central Institute of Professional Training in Obninsk provides physical protection and security force training, as well as equipment support and certification.
- The Moscow Institute of Professional Training is responsible for training the rising nuclear elite, as well as mid- and top-level management, in non-technical disciplines. The Institute was recently designated one of the lead training institutions for nuclear security culture.
- Navy personnel assigned nuclear-security-related duties are trained at the Kurchatov Institute in Moscow and the Kola Technical Center in Murmansk.

---

27. For example, the Department of Physics and Technology at the Tomsk Polytechnic University offers a certificate titled Specialist in Security and Nuclear Materials Nonproliferation. Tomsk Website, <http://tpp.tomskinvest.ru>.

- The Siberian Training and Technical Support Center at the Budker Institute of Nuclear Physics provides MC&A technical support and training to regional sites.
- The Urals Training Center at the All-Russian Scientific Research Institute of Technical Physics, Snezhinsk, and the Technical Support Center perform a function in the Urals region similar to that of the Siberian Training Center in its region.

While on-site training is convenient, training sessions at central locations are usually more effective, since employees are free from their everyday activities and have more opportunity to exchange information and views with their colleagues from other sites. Awareness training is especially important for managers, who have more authority and power than operators and provide other employees with guidance and direction.

Over the past few years a major contribution to MPC&A training has come from the U.S. Department of Energy and its national laboratories. Specifically, DOE's long-term education and awareness project includes a number of initiatives designed to improve the culture surrounding MPC&A. Various MPC&A culture training modules have been inaugurated under the project, as have culture evaluation surveys and a pilot site/facility MPC&A culture coordinator program. These coordinators are expected to initiate and implement security-culture-related projects at the individual facility level. International training projects not only help nuclear security personnel grasp the essence of nonproliferation and their role in improving security, but help them realize that they are not alone in dealing with security problems. A central message is that these problems and approaches are common to nuclear facilities worldwide.

As the International Atomic Energy Agency completes its work on conceptualizing nuclear security culture and develops relevant training guidelines for its members, a major challenge will be to reconcile and integrate national security culture perceptions that are often at variance with one another. Russia is a case in point. Its nuclear sector has taken some steps forward in security culture training according to its own vision and needs. Any internationally approved guidelines, unless sufficiently generic, could lead to a painful readjustment or not be welcome at all.

5.5 Use of Guards

Rosatom is moving toward a more formal recruitment procedure in which vacancies for top managerial positions are publicly announced and job descriptions are posted on its website. At present, many positions at individual nuclear facilities, especially positions pertaining to security, are neither publicly announced nor open to competition. Different facilities have different procedures for recruiting security personnel. While some facilities try to hire college graduates with special degrees in MPC&A, most prefer to offer positions to experts already working at the facility. Medical tests and psychological compatibility tests are generally required of armed guards and protective forces.

Recruitment of a corps of professional departmental guards is a positive new development that could contribute to an improved security culture. In 1999, the federal Law "On Departmental Guards" and the implementing government resolutions authorized a number of federal ministries and agencies, including Minatom, to establish in-house security services. Until recently, security fell to units under the jurisdiction of the Ministry of Defense, the Interior Ministry, and the Federal Security Service.[28] The rationale behind the 1999 law was to assign protective functions to professionals who would be fully responsible to the ministry or agency that employed them, and thus presumably better motivated. A major function of departmental guards, as defined by law, is

to "protect sensitive facilities from unlawful acts." Guards are also tasked with controlling access to these facilities by employees and visitors. They are specially trained to deal with insider threats.

Departmental guards are recruited from among Russian nationals only. A high-school diploma is an absolute requirement. Their pay is funded from the internal budgets of the relevant ministries and agencies, and they are assigned to protect government-owned facilities. They can also be tasked by special contract with providing protective services for joint-stock or other companies involved in sensitive projects that fall under the purview of any ministry or agency. Departmental guards are armed and, if necessary, may use physical force and/or weapons. In extreme situations, they are allowed to use weapons without warning. They can operate outside their facilities, either in hot pursuit or while protecting transport vehicles in transit. Order no. 139 of February 22, 2001, a directive issued by Minatom, established a three-tiered organizational structure for the ministry's departmental guards, consisting of a separate Minatom (now Rosatom) department, regional offices, and protection units assigned to nuclear facilities. Rosatom departmental guards are increasingly taking on responsibility for MPC&A functions. Lack of funding, the incomplete legal and regulatory basis, and inefficient interagency coordination, however, pose major impediments to deploying additional guards at Rosatom or other agencies' nuclear facilities.

As a rule, Interior Ministry troops assigned to nuclear facilities report to superiors both on-site and in the Interior Ministry. Frictions often ensue from this "dual loyalty" syndrome. Interior Ministry personnel participate in developing security procedures at nuclear sites, and they conduct investigations, but they are not formally part of Rosatom. At the same time, facilities protected by these troops are required to fund all of the relevant construction and infrastructure projects, procure equipment, and maintain protective infrastructure for the troops. Professionals who are not encumbered with conflicting responsibilities can establish more efficient lines of communication and modes of cooperation, ultimately improving security standards and engendering a healthier security culture. Another major task is to make the Interior Ministry's military culture compatible with that of the security culture at nuclear sites. Some experts justifiably believe that, without this coordination, interior troops will not be able to perform as efficiently as they should. These troops should be acculturated sufficiently to allow them to coordinate their activities with site security personnel.[29]

28. "On Departmental Guards," Federal Law no. 77-FZ , April 14, 1999, <http://www.referent.ru>.

29. Igor Goloskokov, "Reforming Interior Troops at Russian Nuclear Sites," *Yaderny Kontrol* 4 (winter 2003): pp. 39-51.

In the wake of the 2004 administrative reform, a major challenge for Rosatom and other agencies with jurisdiction over nuclear facilities is to modernize their personnel policies consistent with nationwide economic trends. One step is to replace top managers with purely technical backgrounds with managers imbued with the new, more desirable professional culture. This cultural shift is already apparent in Rosatom itself. With the exception of Anatoliy Kotelnikov, the official in charge of security, most other deputy directors are economic and financial experts. This revolution must be carried to the level of facility directors as swiftly as possible. Tentative plans to turn part or all of some facilities into joint-stock companies make this process even more important. Whatever the case, security culture will prosper if embedded in a more efficient and transparent professional culture. Western and international efforts to spur the emergence of a new professional culture in Russia, however, must incorporate a healthy respect for differences in history and tradition. Otherwise the most well-intended assistance could become counterproductive. ■

CHAPTER VI

MPC&A LEGAL AND REGULATORY FRAMEWORK

A smoothly functioning nuclear regulatory framework is one of the key elements of a high-quality nuclear security culture. Two elements comprise such a framework: well-crafted written directives and a tradition of obedience to law that fosters compliance with these directives. Serious shortcomings in both areas impair Russian nuclear security. A shortage and insufficient scope of guidelines and regulations and a culture that emphasizes loyalty to individuals rather than compliance with rules endanger the security of Russian stockpiles of nuclear material. Although Russia has developed a sizeable body of laws and regulations relating to nuclear safety and security, much remains to be done to extend these directives to encompass all aspects of nuclear security. More importantly, a new attitude towards following procedures and regulations needs to be instilled among the managers, operators, and security guards at Russian nuclear facilities to make the laws and regulations work.

6.1 Current Legal Framework

The umbrella Law "On the Use of Atomic Energy" was adopted in 1995 to establish, among other things, a general framework for material protection, control, and accounting (MPC&A) activities.[1] Article 4 of the Law establishes guidelines for nuclear-materials control and accounting (MC&A). Article 11 sets forth procedures for the physical protection of nuclear facilities, laying out the stages of the fuel cycle that are subject to physical protection and listing the principles by which physical protection shall be organized and implemented. Article 14 provides guidelines for exporting and importing nuclear materials, equipment, and technologies. The Law remains Russia's principal legal document for regulating all aspects of the nuclear industry, including fuel fabrication, trade, the transportation and storage of nuclear materials, and the handling of radioactive waste.

In 1996, the Russian government adopted a "Concept of the Federal System for Nuclear Materials Control and Accounting," which became the principal founding document for nuclear MC&A in Russia. In 1997 the government approved "Regulations for the Physical Protection (PP) of Nuclear Materials, Installations, and Facilities" (revised in 1998), followed in short order by a number of related Ministry of Atomic Energy (Minatom) regulations and documents. On December 1, 1997 the government issued a resolution enacting procedures for developing and approving federal norms and regulations for the nuclear energy sector.

In 2000 the government approved revised "Provisions for Federal Nuclear Materials Control and Accounting," and in 2001 it issued "Main Principles for Nuclear Materials Control and Accounting." In 2002, the government adopted "Procedures for Physical Protection of Radioactive Sources, Radioactive Materials, and Waste." Finally, in late 2003, Russia's Security Council developed "Principles of State Policy on Nuclear Security and Radiation Safety in the Russian Federation for the Period Through 2010 and Beyond," which outline government policy on ensuring nuclear safety and security for the near and long terms.[2] The latter was signed by the president, thereby giving it a status comparable to that of a presidential decree. These documents and other related

1. "On the Use of Atomic Energy," Federal Law no. 170-FZ, November 21, 1995, <http://www.minatom.ru>.

documents established the legal basis and guidelines for nuclear MPC&A activities and policies, both at the Federal Atomic Energy Agency (Rosatom) and at other ministries and agencies that have custody of nuclear materials.

Also contributing to nuclear security are a number of general-scope laws and regulations, including for instance the Law on State Secrets and the Law on Technical Regulation. One difficulty with such laws is that, because they were originally designed to apply to the general industrial sector or the military and security services, they often fail to accommodate the specific requirements of the nuclear sector. For example, the Law on Technical Regulation was suspended from application to the nuclear industry for seven years after it was adopted. It was deemed counterproductive.[3]

However, there are still numerous gaps in the nuclear MPC&A legal basis that directly and indirectly weaken efforts to improve Russia's nuclear security culture. Many federal laws and regulations, especially those applying to the industry and site levels, are either lacking or in need of updating. For example, the nuclear defense complex badly needs the long-overdue Law "On Nuclear Weapons," which would regulate the potential use, storage, physical protection, control, and accounting of Russia's nuclear arsenal and weapons-grade materials. Some federal documents that urgently need to be approved and promulgated include "Federal Material Control and Accounting System for Defense-Use Nuclear Materials" (concept and rules), "Federal Register for Defense-Use Nuclear Materials," "Guidelines for Application of Main Rules for Accounting and Control of Nuclear Materials," "Rules for Accounting and Control of Nuclear Materials during Transportation," and "Revision of Main Rules for Accounting and Control of Nuclear Materials." Of 255 documents and regulations on security and MPC&A recommended by the U.S.-Russian Joint Commission, less than one-third have been developed and approved.[4]

The government recognizes this gap and is taking steps to fill it, though Russian officials remain skeptical about whether the number of directives recommended by their U.S. counterparts represents an optimal package for Russia. The principal guidelines for nuclear security policy for the next few years specify a number of legal and regulatory documents that will be developed and submitted to the Duma for adoption. Among them are bills pertaining to nuclear and radiation safety and security, nuclear defense installations, handling radioactive waste, and the development, operation, transportation, and disposal of nuclear weapons.[5]

6.2 Legal and Regulatory Obstacles

Rosatom is not the only agency in possession of nuclear materials. As mentioned above, the Russian Academy of Sciences, Ministry of Education and Science, Ministry of Transportation, Ministry of Industry and Energy, and Kurchatov Institute, among others, have custody of nuclear materials. Rosatom thus shares the responsibility for nuclear materials, including MPC&A, with other industries and agencies within the executive branch. Rosatom does, however, maintain an inventory of all federally owned nuclear materials.

Although Rosatom has a hand in developing the federal laws and regulations governing the agencies to which nuclear materials have been entrusted, the security norms, regulations, and

---

2. Office of the President, "The Principles of State Policy for Nuclear Security and Radiation Safety and Security in the Russian Federation for the Period Through 2010 and Beyond," Presidential Directive no. PR-2196, December 4, 2003, <http://www.scrf.gov.ru/Documents/Decree/2003/2196.html>.
3. Authors' interview with a Rostekhnadzor official, September 17, 2004.
4. Authors' interview with a Russian nuclear official, Phoenix, AZ, July 14, 2003.
5. Office of the President, "Principles of State Policy for Nuclear Security and Radiation Safety and Security."

procedures for facilities that are not under its direct control are not well-coordinated. They often contain contradicting and confusing requirements. In many cases the requirements of the Federal Information System,[6] industry-level regulations, and federal security norms contradict one another. At times, security-related norms and regulations conflict with non-security-related federal legal norms. A facility cannot, for example, lay off an elderly security guard who fails medical tests because such dismissals are forbidden under current labor law. One example of this conflict of laws occurred at the Zheleznogorsk nuclear facility, where the head of the security guard force was 73 years old yet refused to retire.[7] Such situations pose a major obstacle to a common security culture standard throughout the nuclear sector.

Due to difficulties in interagency coordination–particularly past disagreements between the former Minatom and the former Gosatomnadzor (GAN)–several important federal documents have not yet been approved. For example, a facility which has both weapons-grade and non-weapons-grade nuclear materials has to maintain different documentation for each category of material. Definitions in the federal and agency-level regulations are ambiguous, leaving unacceptably wide discretion for interpretation. (E.g., "a nuclear site" could be interpreted as all sites within one facility, or each particular site.) The regulations also fail to cover some of the more important activities, such as the transportation of nuclear materials between different facilities located within one site.

Similar obstacles have hindered progress toward implementing regulations governing the conduct of departmental security guards. Here again, the legal experts who prepared the law did not engage in interagency discussion with all of the interested parties during the deliberation phase, with the result that some Rosatom departments and federal agencies involved are either unable or unwilling to implement the regulations.

The key problems related to regulatory documents in the Russian nuclear sector can be summarized as follows:

- They are sometimes obsolete and poorly structured, as well as too general, formalized, and lengthy.
- They are pervaded by unnecessary technical jargon that makes them difficult to understand, especially for new categories of workers being integrated into security culture, and blurs the guidance they provide.
- They were designed to describe technical minutiae rather than providing solutions to problems likely to be encountered by the workforce.
- They lack specific and detailed algorithms for handling fissile-material security and carrying out other critical tasks.

A recent survey attests to the problems with the written instructions supplied to nuclear security personnel. Only 10 percent of nuclear facility employees working with nuclear materials considered the instructions to be clearly written; only 15 percent could list specific security-related "procedures" and "instructions"; and more than two-thirds (68 percent) maintained that many of the existing instructions and manuals were obsolete.[8]

---

6. Rosatom nuclear industry-wide information database (federal nuclear register).

7. Authors' interview with a manager at Siberian Chemical Combine, Phoenix, AZ, July 14, 2003.

8. Survey prepared by an Institute of Physics and Power Engineering training center, cited in Irina Koupriyanova, "Assessment of Effectiveness of U.S. MPC&A Assistance to Russia," *Yaderny Kontrol* 2 (March-April 2002): pp. 57-65.

In a public opinion poll in 2003, respondents were asked to choose one of two reasons behind Russians' noncompliance with legal norms: a lack of respect for the law, or a valid justification for violating the law. Twenty-two percent of respondents chose the first option and 68 percent the second. Respondents found poorly drafted laws to be a valid reason to ignore the law.[9]

Ambiguous instructions and gaps in procedures compel nuclear personnel to make decisions on their own. Errors and miscalculations are a frequent result, creating an environment in which a healthy nuclear security culture is difficult to attain.

6.3 Russian Legal Culture

Russian society has a long tradition of "legal nihilism," meaning disrespect for legal norms, a disbelief in the power of law, and an overall disinclination to obey the law. This is directly related to the Russian traditions of autocratic leadership and arbitrary rule. Many Russians consider direct or indirect orders or favors from higher-ups, not laws and regulations ordained by the nation's political authorities, to be the real rules governing their society. But personal edicts of the kind to which Russians are accustomed are not legally binding and are subject to constant change. The resulting flux undermines respect for the law.

Russia's authoritarian, and then totalitarian, political systems implied that law was created by individuals who were exempt from its effect. Initially it was the tsar who was above the law in the eyes of Russians. He wielded absolute power. His word was the law for everyone, including the highest-ranking nobles in the court. After the revolution of 1917, the Communist government created a legal system which in theory applied to all citizens but in reality exempted political figures and the party leadership to a certain extent. Top Soviet leaders had the final say in matters of guilt and innocence. This arrangement was most visible under Stalin's rule, when even senior party officials could be prosecuted for alleged crimes without due process and no ordinary citizen was safe from persecution. Ideological and political expediency trumped the rule of law.[10]

Despite abundant reporting to the contrary during the 1990s, ordinary people still see the legal mechanism as a repressive rather than a protecting hand. Responding to survey questions, more than half of Russian respondents said that the Russian president should be a powerful master of the country and that respect for government should be grounded in fear.[11] Thus Russia continues to exhibit all of the characteristics of legal nihilism: a prevailing negative attitude toward existing norms, a perception that these norms are unjust, and a lack of desire to build relations among members of society based on established, written legal norms.[12]

Although the nuclear industry was formerly led by a well-educated social elite, legal nihilism has exerted a deleterious influence on the professional culture even there. Russian professional culture defines the relationship between management and employees not in collegial terms but in terms of "leader" and "subordinate." Leaders/managers, not abstract legal precepts, embody legal authority and are perceived to have the moral–though not legal–right to override procedures and regulations within their domain. Thus, nuclear facility managers are rarely challenged by their

---

9. Public Opinion Foundation, Public Opinion Poll, January 24, 2003, <www.fom.ru>.

10. Natalia Varlamova, "Legal Nihilism in Russia: Past, Present, Future," *Sravnitelnoye Konstitutsionnoye Obozreniye* 1 (2000), <http://www.ilpp.ru>. See also Olga Gulina, "Sources of Russian Legal Nihilism," <http://www.uic.bashedu.ru/str_n_col/vestnic/2/gulina.html>, and V. Tumanov, "Legal Nihilism and Its Historical and Ideological Roots," *Gosudarstvo I Pravo*, 1993, <http://ufnovgu.narod.ru/tgp/lituma2.htm>.

11. "Authoritarian Syndrome of Russian Society," *Wall Street Journal*, March 17, 2004.

12. Varlamova, "Legal Nihilism in Russia."

subordinates if their instructions contradict federal law or regulations issued by the federal agency that has jurisdiction over the facility.

Recent years have witnessed some improvement in this situation. Some progressive lawmakers and government officials have worked earnestly to change the outlook of Russians toward the rule of law. The influx of a youthful, less indifferent generation of employees in the nuclear sector and across the industry has also helped. During a recent poll in Russia, for instance, 78 percent of respondents stated that a failure by government officials to abide by laws and regulations was the main problem undercutting respect for the law in Russian society. Asked to choose from a list of 18 principles that should guide government activity in Russia, respondents ranked "following the Constitution" (70 percent) and "civilian control and law obedience" (58 percent) most important.[13]

One important attempt to change attitudes within the federal workforce came in the draft Code of Conduct for Civil Servants in the Russian Federation, which was developed by a group of deputies in 2002. Although the draft went through two readings in parliament and underwent several revisions, it has not yet been adopted. The federal administration developed its own concept, embodied in a presidential decree of August 12, 2002, no. 885, "On Adopting the General Principles of Conduct for Civil Servants." These documents define the legal status of civil servants/federal employees, explain the relationships between these employees and federal bodies, and demand strict compliance with legal requirements. Russia's administrative reform effort, launched in March 2004, was designed to incorporate measures that ensured the primacy of law in the conduct of government officials.[14]

All of these legal efforts must succeed in order for a vibrant security culture to take root in the Russian nuclear sector. As outlined above, the Russian government has made some progress toward encouraging obedience to the law among the general public and within the government. A number of government initiatives have sought to ensure that regional law and regulations, as well as industry standards and procedures, conform to the Russian constitution and federal law. Government officials and other observers, moreover, have come to understand Russians' indifference toward the law and have set out to modify public attitudes toward the role and functions of government. These attitudes seem to be shifting in the right direction with the passage of time, providing some grounds for optimism about the future of law obedience and nuclear security culture in Russia. Until the larger society begins to prize obedience to written directives, the nation's nuclear sector will continue to suffer from the maladies identified in this chapter. ■

13. Tatyana Kutkovets and Igor Klyamkin, "New People in an Old System," Liberal Russia Foundation, September 2002, <http://www.liberal.ru/sitan.asp?Num=258>.

14. Office of the President, "On the Federal Program 'Reforming the Civil Service in the Russian Federation (2003-2005)," Presidential Decree no. 1336, November 19, 2002.

CHAPTER VII

ENFORCEMENT AS DETERRENT

While the "carrots" of encouragement and incentives are essential to improving personnel performance and the overall health of Russian security culture, the "sticks" represented by efficient enforcement of norms and rules are the reverse–and equally crucial–side of motivation. Personnel obey rules and norms not only because they recognize them and understand their importance, but because they fear being punished if they fail to comply. In other words, enforcement should work as a deterrent. Prospective violators should understand in advance that retribution is unavoidable and that infractions will be publicly discussed in the workplace and the media, allowing others to draw the lesson. The optimal balance between carrots and sticks derives ultimately from an assessment of national traditions and history, economic reality, and the conditions peculiar to each workplace or organization.

7.1 Legal Provisions

Eight articles in Russia's Criminal Code, which was drafted and approved in 1996, levy legal sanctions for cases involving breaches of nuclear security and/or diversions of nuclear material:

- Article 188, which pertains to smuggling, imposes penalties ranging from three to ten years' imprisonment for smuggling weapons of mass destruction (WMD), nuclear and radioactive materials, equipment for producing WMD, or other military hardware. Those found guilty of repeated acts of smuggling are subject to prison terms ranging from three to five years, or five to ten years for offenders found guilty of abusing their official power.
- Article 189, which pertains to export controls, imposes penalties ranging from three to seven years' imprisonment for illicit exports of information, equipment, or materials which could be used to produce WMD.
- Article 205 stipulates a life sentence for terrorism using nuclear or radioactive materials or radioactive sources, or for encroachment on nuclear facilities.[1]
- Article 215 imposes a penalty of up to three years' imprisonment for safety and security violations at nuclear facilities–up to ten years for cases with severe consequences.
- Article 220 authorizes prison terms up to two years for cases involving illegal handling of nuclear or radioactive materials (acquisition, storage, use, or transfer)–up to ten years for cases with severe consequences.
- Article 221 stipulates a penalty of up to ten years' imprisonment for cases relating to the theft or extortion of nuclear or radioactive materials.

---

1. In July 2004 President Putin signed a federal law amending Article 205 of the Criminal Code, toughening punishment for acts of terrorism. The new amendment stipulates a life sentence (instead of ten to twenty years of imprisonment) for terrorism using nuclear or radioactive materials or radioactive sources, or encroachment on nuclear facilities. ITAR-TASS, July 26, 2004.

- Article 225 imposes penalties ranging from three to seven years' imprisonment for security breaches involving weapons of mass destruction, WMD-related materials, or equipment that could be used to produce WMD. Personnel found guilty under Article 225 may also be forbidden to hold certain sensitive posts for up to three years.
- Article 226 authorizes penalties of five to ten years' incarceration–up to fifteen years in cases with severe consequences–for theft or extortion of weapons, munitions, explosives, or explosive devices, including nuclear weapons and material.
- Article 355, which discusses the unlawful production and proliferation of WMD, imposes jail terms ranging from five to ten years.[2]

The punishments authorized in the Criminal Code may appear too lenient from the vantage point of the post-9/11 and post-Beslan era. Indeed, in some instances the Code imposes more severe punishments for thefts of conventional weapons and munitions than of nuclear and radioactive materials. There are grounds to believe that President Putin's post-Beslan plan of action will toughen these penalties across-the-board.

Additionally, three articles in the Administrative Code authorize civil punishment for nuclear security violations and diversions:

- Article 9.6, which covers violations of the norms governing the use of nuclear energy and accounting procedures for nuclear and radioactive materials, imposes the following penalties: A private individual may be fined an amount not to exceed 20 times his or her monthly salary, an official may be penalized up to 40 times his or her monthly salary, and a legal entity may be fined up to 400 times its monthly earnings.
- Article 20.19 provides for a fine of up to 10 times the monthly salary for an individual found to have violated security or access procedures at a nuclear closed city.
- Article 20.17 provides for a fine of up to 5 times the monthly salary for an individual found to have violated admission procedures at a guarded facility.[3]

Inspections by the national oversight service have brought pressure on facility managers to enforce rules and standards. As part of the 2004 administrative reform, Russia created a single, integrated Federal Service for Environmental, Technical, and Nuclear Oversight (Rostekhnadzor) to conduct such inspections. Some of these assessments, known as operational inspections, cover MPC&A activity. Noncompliance is punished depending on the severity of the infraction. Fines may be levied, licenses suspended or revoked. One hundred sixty-seven operational inspections were carried out between April and June 2004, resulting in numerous investigations and other corrective actions.[4] Another body empowered with oversight functions is the Prosecutor General's Office, which among other things has a mandate to inspect security conditions at nuclear facilities. The office can launch such inquiries in response to tips received from anonymous sources such as whistle-blowers. In 2004, for example, inspectors visited several nuclear power plants, detecting serious deficiencies in the security precautions at these plants.[5] Inspections by the Prosecutor

2. "Criminal Code of the Russian Federation," 1996, <http://www.d-sign.ru/uk/uk.htm>.
3. "Code on Administrative Offenses of the Russian Federation," 2001, <http://www.rg.ru/oficial/doc/codexes/APK/>.
4. "Statement of GAN Oversight Activity from April to June 2004," GAN Website, <http://www.gan.ru/org>.
5. "Deficiencies in Security Standards of Several Nuclear Power Plants Have Been Identified," *RIA Novosti*, October 28, 2004, <http://www.rian.ru/rian/intro>.

General's Office are deemed to complement the Rostekhnadzor mandate by focusing on safety- and security-related administrative and criminal violations. Nuclear security culture tends to shape up within an organization in anticipation of such inspections. Preparations factor in the lessons-learned from past inspections.

7.2 Investigation Procedures

The criminal investigation departments of the Federal Security Service (FSB) and the Ministry of Interior Affairs (MVD) work with civilian or military prosecutors, respectively, to investigate cases involving the diversion of nuclear materials. Which agency conducts an investigation depends on the circumstances, people, and materials involved in the case. Rosatom works with the security personnel assigned to individual facilities to carry out internal investigations, keeping Rostekhnadzor informed. Other agencies and bodies are kept abreast of the progress of an investigation, depending on the severity of the case.

Interior Ministry guards who detect an act of diversion usually report to the Interior Ministry and/or the head of shift at the site, depending on the gravity of the breach of security and other circumstances. The latter informs the Rosatom department to which the site reports, as well as Rostekhnadzor, and sometimes the FSB. This reporting procedure is cumbersome, involving as it does several agencies that do not coordinate their efforts effectively and, indeed, sometimes compete with one another. The procedure needs streamlining and further refinement.[6] Rosatom departmental guards are gradually replacing Interior Ministry troops, a move that will rationalize the procedure to some extent. (The guards and the facility do report to the same agency, Rosatom.)

Efforts are underway to further improve the reporting procedure. On December 3, 2002, for example, the Prosecutor General's Office issued Order no. 70, laying out procedures for special reporting on emergency situations and crimes. According to the order, prosecutors must immediately inform the Prosecutor General's Office about all emergencies at nuclear facilities. The Prosecutor General's Office informs the FSB or the MVD about the results of investigations and decisions made.

The FSB's mandate and authority were expanded under a presidential decree on "Provisions of the Federal Security Service of the RF," issued July 11, 2004 in conjunction with the administrative reform. The decree bestowed new authority and functions on the FSB. The service's investigative powers in particular grew significantly under the decree. Even the new, streamlined procedure envisioned in the decree, however, might be hampered by the different organizational and professional cultures of the agencies involved. Different perceptions of major threats and the best methods of coping with them could continue to pose a severe impediment. In a post-Beslan decree of September 13, 2004, President Putin made improving coordination among Russia's security and law-enforcement services a high priority.[7] At a cabinet meeting on the same date, he discussed integrating those services to establish a single counterterrorist center.[8] These actions could yield more effective interagency coordination in the realm of nuclear security.

---

6. Authors' interview with Russian nuclear experts, July 12, 2003.

7. Office of the President, "On Urgent Measures for Improving the Effectiveness of Combating Terrorism," Presidential Decree no. 1167, September 13, 2004.

8. Vladimir V. Putin, "Address of President Vladimir Putin to the Cabinet Meeting, September 13, 2004," <http://www.kremlin.ru/text/>.

7.3 Vague Reporting Practice

The official diversion statistics are rife with discrepancies. In September 2000, while briefing journalists about diversions of nuclear material, then-First Deputy Minister of Atomic Energy Valentin Ivanov claimed that there had been 23 attempts at diversion in Russia in 1991-2000 (21 in 1991-1995, and 2 after 1995). In 1998, by contrast, Nikolai Redin, then the deputy director of the Ministry of Atomic Energy (Minatom) department of information, materials, and facilities protection, made reference to about 30 cases of diversion at Minatom facilities in 1992-1995.[9] In 1999, Victor Yerastov, a representative of the same Minatom department, said that there had been about 52 cases of radioactive material diversion, of which 25 had involved nuclear materials.[10]

Of 127 cases of actual or attempted diversion of nuclear and radioactive materials reported by Minatom to the International Atomic Energy Agency (IAEA) from 1993-2001, the material was declared to have been retrieved in 10 cases; diversions were declared to have involved criminal intent in 13 cases; and diversions were declared to have involved organized crime in 4 cases.[11] The cases reported to the IAEA Illicit Trafficking Database included unauthorized acquisition, provision, possession, use, transfer, or disposal of nuclear material and other radioactive substances. Over the past decade, about 600 illicit incidents were reported worldwide.[12] The Los Alamos National Laboratory (LANL) database on nuclear diversions mentions 189 similar cases involving nuclear materials in Russia.[13]

What explains the varying figures given out by Russian officials? There are grounds to believe that not all incidents were reported by Minatom or recorded in the databases. Rosatom and other governmental agencies often provide conflicting information. For example, Minatom denied cases of diversion at its Luch Scientific Production Association, even after an investigation had commenced and the person charged with the theft had publicly admitted guilt.[14] Another example might include the attempted theft of 18.5kg of nuclear material from a facility in the Chelyabinsk region. The case was publicized at a December 1998 press conference by the MVD's Major General Valeriy Tretyakov, who was reportedly reprimanded for disclosing this information.[15] Minatom officials vehemently denied the incident until it was finally confirmed by Victor Yerastov of the Minatom department of information, materials, and facilities protection.

Rosatom officials also tend to portray known cases not as actual diversions but as attempted diversions. By definition, diversion is the act of moving nuclear material out of the material balance area. The concept of an *attempted* diversion is more ambiguous. It typically remains unclear from official statements at what stage an attempted diversion was prevented: at the conceptual and planning stage or during implementation, when the materials were already in possession of the perpetrators. Whether the material was moved out of the material balance area, out of the facility entirely, or just misplaced also remains hazy in many official accounts of these incidents. The vague definition of an attempted diversion makes it difficult to apply investigation and enforcement procedures and levy penalties against violators. This fact helps explain the discrepancies between

---

9. Oleg Lebedev, "There Were No Nuclear Diversions in Russia in the Last Three Years," *RIA-Novosti*, October 28, 1998.

10. Victor Yerastov, interview with *Yaderny Kontrol* 6 (November-December 1999): pp. 40-43.

11. Authors' interview with a Rosatom official, February 7, 2002.

12. "In a Bid to Prevent Nuclear Terrorism, UN Agency Tracks Illicit Trafficking," UN Website, September 23, 2004, <http://www.un.org/apps/news/>.

13. Stacey Eaton, "Tracking Nuclear Smuggling: Identifying Trends and Patterns," Paper Presented at the 43rd Annual Meeting of the Institute for Nuclear Material Management, Orlando, FL, June 23-27, 2002. The database includes several types of materials: uranium, plutonium, radioisotopes, dual-use materials, neptunium, americium, and thorium.

14. Public Broadcasting System, "*PBS Frontline*: Loose Nukes," 1996, <http://www.pbs.org/wgbh/pages/frontline/shows/nukes>.

15. "NIS Nuclear and Missile Database," Nuclear Threat Initiative Website, <http://www.nti.org>.

Rosatom statistics and the data provided by other organs, particularly the enforcement agencies.

More recently, Rosatom has been demonstrating increasing reluctance to acknowledge that Russia's nuclear sites are vulnerable and that violations have taken place. In September 2004, for instance, Rosatom Director Alexander Rumyantsev publicly stated that, over the past 25 years, as little as 100kg of non-weapons-grade natural uranium had been stolen in Russia, while the quantity of weapons-grade uranium stolen was measured in tens of grams, all of which had been located and recovered.[16]

Information from the oversight service (now Rostekhnadzor) and the Ministry of Internal Affairs usually does not clarify the situation. These agencies often provide a total number of people under investigation and convicted, but these figures generally are not broken down by specific case to indicate how severe were the sentences imposed. More transparency and public information are required if a healthy nuclear security culture is to materialize in Russia.

7.4 Poor Prosecution

Poor enforcement results from a culture that does not encourage reverence for or obedience of the law. The cultural problem continues to bedevil a range of different industries and activities, not just those related to security. As mentioned in Chapter VI, laws in Russia are sometimes applied selectively to suit the immediate interests of the political elite; violators thus are only arbitrarily prosecuted. For example, in the area of export control, a subject of persistent U.S. concern, about 90 allegations of wrongdoing were investigated in 2000-2003. Only three cases resulted in publicly reported criminal convictions, with the rest being dropped for reasons not disclosed to the public.[17]

Corruption among law-enforcement officers is widespread, adding to the problem of lax enforcement. Indeed, according to a January 2002 survey of the Russian public by the Public Opinion Foundation, Russians view enforcement bodies as the most corrupt arm of government in their country. One of the principal aims of the ongoing reform of the judiciary is to reduce corruption. Several high-profile cases involving enforcement officers bear witness to the government's determination to root out corruption.[18] The Russian Ministry of Interior Affairs has acknowledged the existence of corruption in the enforcement agencies and sought to fight it. Still, despite the healthier corporate culture in Russia's nuclear sector as compared to other industries, the abundance of costly materials, including radioactive substances over which there is inadequate accounting and control, leads inexorably to corruption and crime.

Another factor contributing to poor enforcement is the low level of professionalism among Russian enforcement officers compared to the private sector. Since experienced individuals with legal backgrounds are in great demand and well-paid in Russia's private sector, many experienced professionals have left federal agencies for private enterprise. One result is apathy toward the diversion and theft of state-owned fissile material.

Court officials and officers have a reputation for going easy on violators. For example, an employee of the Elektrostal Machine-building Plant in Moscow oblast who diverted 115kg of uranium pellets from the facility in 1993 was sentenced to only four years in prison. Even this modest

16. "Over 25 Years, 100kg of Uranium Has Been Stolen in Russia," Newsru.com, September 16, 2004, <http://newsru.com/Russia>.

17. Authors' interview with Sergey Mikhailov, deputy head of export control department at Ministry of Economic Development and Trade, December 14, 2003.

18. For example, the 2003 case of "policemen-werewolves" accused of bribery and covering up illegal activities. "Policemen-Werewolves Were Engaged in Smuggling for More Than $1 Billion," *Vremya Novosti*, April 23, 2003.

jail term was later suspended. The judge portrayed the suspension as an act of compassion toward the defendant, who reportedly had three children, earned a meager salary, and thus was driven to improve his financial status by selling uranium.[19] In many cases, moreover, facility management seems more interested in getting reimbursement for stolen items under the Administrative Code than in initiating time-consuming criminal investigations and publicizing these punitive measures as a lesson to other potential offenders.

Another example of lenient punishment involved the diversion of isotopes at the closed city of Lesnoy, when only one of several participants was prosecuted. (See Appendix II.) In still another case, criminals who attempted to sell U_{235} at Balashikha in Moscow oblast in December 2001, but were apprehended by law-enforcement agents, were sentenced to only one year of imprisonment. Again, the jail term was suspended.[20] Investigative practices and the courts' performance have started to improve somewhat. In April 2004, for instance, the Tomsk Federal Security Service office reported that it had completed its investigation of Siberian Chemical Combine employee Anatoly Samtsov, who was charged with "nuclear and radioactive materials thefts using official power" under Article 221 of the Criminal Code. On this occasion the FSB shared information about the incident with the public. Court proceedings were to be initiated before the end of 2004.[21]

Informing potential offenders about the legal repercussions associated with diversions of nuclear material is one effective deterrent to future diversions. Over time, if the government moves aggressively against offenders, the publicity accorded these cases should help improve the security culture at Russian sites. The number of diversions and attempts at diversion decreased slightly by the end of the 1990s, not only because of improved security equipment, but also because of increased salaries and motivation, better security discipline at the facility level, and growing public awareness of the danger represented by the black market. If the Russian media initially paid little attention to diversion cases and criminal investigations, numerous media outlets have covered recent cases such as the December 2001 diversion case in Balashikha and the diversion of radioactive materials and uranium by Atomflot Deputy Director Alexander Tyulyakov in October 2003.[22]

While the national media have provided better and more comprehensive coverage of these incidents, the regional media have not performed as well. The relative dearth of regional scrutiny is attributable largely to a lack of awareness and competence among journalists, the fact that the doings of local nuclear facilities take place out of the public eye, and restrictions on freedom of the press. Better public outreach and enforcement would be important vehicles for strengthening the security culture at these sites.

Enforcement of laws and regulations has always been a problem in Russia. Given the mentality of Russians, which was shaped by a long period of ruthless totalitarianism, enforcement and punishment will unfortunately remain an important tool to instill security culture. For the time being, there is a serious gap between what is on the books and what can be realistically expected to be implemented. As the situation improves, more emphasis must be placed on internal monitoring and control. As with other security-culture-related arrangements, more transparency and public outreach are a must. ■

19. "People Involved in Uranium Smuggling Sentenced in Electrostal," *Prestupnost I Bezopasnost*, November 15, 1997, p. 4.

20. Oleg Sultanov, "Sellers of Uranium Were Penalized," *Moskovskiy Komsomoletz*, December 4, 2002, p. 3.

21. "Siberian Chemical Combine Employee Is Charged for Radioactive Materials Theft," Rusmet.ru, April 13, 2004, <http://www.rusmet.ru>.

22. Nick Walsh, "Nuclear Shipyard Director Held for Uranium Hoard," *The Guardian*, October 1, 2003.

CHAPTER VIII

CONCLUSIONS

The United States and other nations[1] have invested significant resources in a bid to enhance the security of nuclear facilities in Russia. Most of this funding has gone toward providing equipment, hardware, and relevant services to improve material protection, control, and accounting (MPC&A) systems at Russian sites. As extensive evidence suggests, however, too little has gone into efforts to nurture security culture among the personnel who operate these systems. Security culture is no panacea, but it should be recognized as an essential ingredient for effectively reducing nuclear dangers–especially for Russia. Accordingly, Russia's nuclear sector will continue to require not only technological innovation, but also the cultivation of knowledgeable, skilled, and motivated personnel who are trained to use modern equipment and adhere to best practices.

A variety of management and learning tools can help produce such a workforce. Given the increasingly multifaceted nature of the threat, as attested to by the recent surge in terrorist activity on Russian soil, the effort to bolster security culture must ultimately go beyond the nuclear facilities specified in this report. Organizations that transport nuclear materials and organizations that use radioactive sources could benefit from the recommendations set forth here. Although these organizations are structured somewhat differently from nuclear facilities, the underlying assumptions and principles are the same with respect to security culture.

Unless the Russian government embraces this idea and commits itself to augmenting nuclear security culture as part of an improved overall professional culture, any efforts undertaken by the West will yield limited results at best. No matter what joint strategy Russia and the West pursue, it must be clearly understood that Western experience and standards cannot be transplanted wholesale to Russia, which is undergoing rapid political and socioeconomic changes. To be successful, this strategy must take into account differences in work culture and traditions. It must also take into account the unique role played by the human factor in protecting nuclear material in Russia.

How can the West best contribute to this process, and what would be the optimal role for Russia? It is important to recognize that, after more than a decade of painful transition, Russia is on the verge of becoming a "normal," middle-income capitalist economy.[2] That said, this rapidly evolving process has not yet contributed to better security inside the country. Also, the nation's economic and political institutions remain far from perfect. To characterize Russia as a normal middle-income country is not to overlook the messiness of its politics and economics or its peculiar patterns of leadership. However, many of Russia's problems are typical of countries at a similar level of economic development. Most democracies in this category are rough around the edges. Their governments suffer from corruption, their judiciaries are politicized and often ineffective, and their freedoms of the press and public expression are incomplete. One common feature for most of these countries–Russia being no exception–is that the people's mentality often lags behind new economic and other realities. Political leaders must work proactively to bring public attitudes and habits in line with these new realities, especially in priority areas such as nuclear security. Only thus can they curb present and emerging threats.

---

1. In addition to the United States, Canada, the European Union, Germany, Finland, Sweden, and the United Kingdom have contributed or committed funding to improve Russia's MPC&A.

2. Andrei Shleifer and Daniel Treisman, "A Normal Country," *Foreign Affairs*, March/April 2004.

The Model of Security Culture Mechanism laid out in Chapter I, Figure 2, spells out the tasks that must be performed to instill security culture within an organization. As in any generic model, most of the items listed under the four headings–Leadership, Proactive Policies and Procedures, Personnel Performance, and Learning and Professional Improvement–need to be evaluated against the backdrop of national experience and adjusted to Russian realities. The scope of these categories, moreover, goes beyond the security mission, implying improvements to the nation's overall professional culture. In other words, better security culture comes in part as a product of better professional culture across-the-board. But in return it provides benefits not only in security terms, but also in safety, productivity, and general management. This is especially true now that terrorism in Russia is becoming more radicalized. Ideally, then, the efforts and time sunk into developing security culture will yield benefits all around.

Development of a healthy security culture is a time-consuming process, but in the short-term perspective there are several specific actions that Russia should take, either by itself or in cooperation with the West:

- **Increase funding for security arrangements**. Windfall revenues from oil and gas exports produced a surplus for the FY2004 budget. The government, consequently, could easily boost spending on security measures. In his 2004 state-of-the-union address, President Vladimir Putin estimated that Russia's GDP would double in the next 10 years. In August 2004, top officials claimed that Russia had a chance to catch up with Spain, South Korea, Greece, and other comparable countries by 2005 in terms of purchasing power.[3] If these ambitious plans come to fruition, leaving Russia in the $8,000-$10,000 per capita bracket, the country can be expected to begin looking after its own security needs consistent with its newfound prosperity. Another sizable increase in security spending would be feasible. From a short-term perspective, the government's plans to raise the 2005 defense and security budget and allocate more money to counterterrorist activities are likely to build political momentum toward more federal spending on nuclear security. New national investment in security upgrades at nuclear sites would send a positive signal to the personnel who operate these sites, bolstering their morale. President Putin has personally acknowledged that Russia has not been spending as much on nuclear security as it should, and that it needs to reverse its dependence on foreign funding in this sensitive area.[4]

- **Invigorate the role of the Federal Assembly**. In reaction to the Beslan tragedy, both the State Duma and the Federation Council became involved in drafting relevant laws and amending existing laws. Though these legislative initiatives rightly focus on measures such as protecting people from acts of terrorism, compensating for damage and injury, and regulating migration, lawmakers also need to provide a solid legal basis for protecting weapons and materials of mass destruction, nuclear facilities, and hazardous sites. To this end, Russian legislators stand to benefit from the experience of their counterparts in other countries, especially the United States. More legislative exchanges and information sharing would be helpful.

- **Introduce more transparency**. Excessive secrecy in nuclear security is counterproductive, because culture depends on shared attitudes and habits, and thus on a shared understanding

3. Aleksei Vinogradov, "A Promise to Russians to Get Rich," RBC News, August 12, 2004.

4. Office of the President, "The Principles of State Policy for Nuclear Security and Radiation Safety and Security in the Russian Federation for the Period Through 2010 and Beyond," Presidential Directive no. PR-2196, December 4, 2003, <http://www.scrf.gov.ru/Documents/Decree/2003/2196.html>.

of threats and responses. Compartmentalization, then, works against security culture. Over the past year or so, the government has repeatedly resolved to make basic information about its operations available to the public. It failed to carry out most of these resolutions. One example is government resolution N-98 of February 12, 2003, which instructed government bodies to provide a much wider range of information about their activities. The resolution listed specific categories that should no longer be off-limits to the public. Had it been implemented as required by February 2004, the public would have been apprised of the status of programs, budget allocations, foreign assistance programs, and a range of other government activities. Knowledge about activities formerly shrouded in secrecy will exert a calming and mobilizing influence on the public–supporting security culture in the nuclear complex while allowing citizens to hold their representatives accountable.

- **Accelerate nuclear security programs**. The urgency of the task of protecting nuclear material requires immediate action. Promoting security culture will be far more difficult if the government does not push its security upgrades aggressively. The "Principles of State Policy on Nuclear Security and Radiation Safety in the Russian Federation for the Period Through 2010 and Beyond" document approved by President Putin in December 2003 envisions introducing a "unified protection system for nuclear and radioactively dangerous facilities and material" in two phases, 2004-2005 and 2006-2010.[5] To be sure, this is a time-consuming process, but it could be accelerated dramatically given sufficient resources and presidential attention.

- **Make the legal basis more comprehensive and instructions more user-friendly**. The more complete the laws and regulations governing nuclear security, the less room personnel will have to improvise and, perhaps, make mistakes. The drafters of these directives cannot foresee every threat to nuclear security. However, clear, concise laws and regulations will help the personnel entrusted with nuclear security act in accordance with national policy when unforeseen events do occur. Russia needs to fill the gaps in its legal framework, but it should do by developing instructions and regulations that are brief and solution- rather than process-oriented. This will cut down on popular resistance to nuclear security directives. To enable these instructions to address specific problems, and to instill security culture, the personnel who will carry out the instructions should be enlisted to help prepare them. Not only would this tap their technical skills, but it would also give them a sense of ownership and help them understand the rationale behind procedures that might seem redundant or unduly cumbersome. Once these individuals have been briefed on the instructions, strict adherence and implementation become the key element in assuring security.

- **Expand independent monitoring and oversight**. In May 2004 an integrated oversight service–the Federal Service for Environmental, Technological, and Nuclear Oversight, or Rostekhnadzor–was created, absorbing the Federal Nuclear Oversight Agency (GAN). Rostekhnadzor needs to continue and expand its so-called operational inspections, which evaluate the security features at various nuclear facilities. The leadership of Rostekhnadzor needs to prevent the interests of the service's nuclear component, the smallest of its three components, from being drowned out by other priorities. Independent monitoring and inspections are a powerful tool for raising standards of security culture and instilling professional discipline. To that end, the MPC&A Operations Monitoring (MOM) Program, a venture sponsored by the U.S. Department of Energy, performs a similarly useful function. The MOM Program is designed to monitor critical MPC&A processes and procedures at Russian sites, assuring U.S. and Russian team members that U.S.-funded systems are operating properly. MOM systems have been installed at four non-

5. Office of the President, "Principles of State Policy for Nuclear Security and Radiation Safety and Security."

Rosatom sites, and four more sites are expected to join the program before long. Rosatom must embrace this program as well.

- **Focus training on security culture**. For nuclear security culture to take hold at the facility level, top managers must take the lead. In Russia, as we have seen, the preferences of high-ranking officials carry tremendous weight. Managers must embrace the requisite mindset and beliefs, communicate these beliefs to their subordinates in word and deed, and perform their duties in accordance with best management practices. A special training package for senior managers, then, would be a vital step toward cultivating security culture throughout the nuclear sector. Such a package would cover nonproliferation, MPC&A, and personnel management. Simulations would be a useful way to convey the necessary concepts. Supplemental training programs, broken down into specific modules and tailored for each target group in the organization, would help cement these concepts and make security culture more sustainable. (See description in Appendix II.)

- **Encourage a system of incentives for personnel**. Since more funding will presumably become available, a mechanism of incentives must be introduced to help attract more young, well-educated Russians to posts in the nuclear sector, develop positive attitudes toward sustaining MPC&A equipment and using it consistently, and make security-related jobs prestigious and career-enhancing. As Rosatom conducts annual competitions among nuclear facilities to choose the best enterprise of the year in terms of product quality and management performance, it should incorporate the elements of security culture into its list of selection criteria. In view of the dramatic salary increases for military and security personnel announced in September-October 2004, it seems reasonable to also substantially increase the bonuses granted personnel with access to nuclear materials. Bonuses might rise from the current 20 percent of the annual salary to 50 percent, or even more.

- **Introduce a system of external evaluation and self-assessment**. Since culture in general evolves slowly and resists change, the nuclear security culture will need periodic reevaluation to check on the effectiveness of corrective action and detect emerging concerns. Rosatom and other agencies must make self-examination mandatory by instructing facility managers to perform periodic assessments of nuclear security culture. They should periodically remind top managers that the culture needs to show progress and that cultural change requires their personal initiative and support. Their own personnel evaluations, promotions, and pay raises should be keyed to improvements in security culture. (See Appendix III for generic evaluation methodology).

- **Develop public awareness programs**. The "public chamber" suggested by President Putin in September 2004, as well as other public outreach programs, should address the relevant nuclear security issues. Target groups for these programs would include both the general public and nuclear professionals who work outside the area of nuclear security. The public can be made aware of the importance of nuclear security in two ways. First, connecting the security of nuclear and radioactive materials with environmental safety–a matter of public concern ever since the Chernobyl accident–would imprint the importance of security on the popular mind. Second, making the link between nuclear security and terrorist incidents would persuade the public to rally behind nuclear security. A public outreach campaign would target institutions such as regional universities, regional media and decisionmaking bodies, trade unions, and churches. The Russian Orthodox Church seems willing to play a role in Russia's antiterrorist drive and to address other important issues. People working within the nuclear industry need to ensure that whatever information about nuclear security they communicate to the general public is

clear and accurate, lest the industry be perceived as evasive or dishonest. Such perceptions would cloud both the public reaction and the organization's internal nuclear security culture. Conversely, a demonstrated willingness to inform the public about nuclear security would benefit the internal culture.

A supportive international environment would facilitate the efforts undertaken by Russia and other countries to promote security culture. To this end:

- The G-8 should discuss security culture at its annual summit meetings. Russia, which is scheduled to host the summit in 2006, should explicitly request the G-8 countries to promote this concept and to include this item on the agenda.
- International MPC&A assistance to Russia under the G-8 Global Partnership Against the Spread of Weapons and Materials of Mass Destruction is another vehicle to raise the visibility of security culture. Western donors should rally behind the U.S. Department of Energy's focus on security culture and work to optimize Russia's human factor.
- The International Atomic Energy Agency should consider throwing its own weight behind these efforts by developing an internationally acceptable concept of nuclear security culture and launching appropriate information sharing/training programs in selected countries.
- UN Security Council resolution 1540, which directs UN member states to rein in the spread of weapons of mass destruction, can play a useful role in bolstering nuclear security culture. If member states were required under its reporting provisions to submit information about their efforts to cultivate security culture among nuclear personnel, they would begin to accord this concept the priority it deserves.

What does the future hold for Russia, a geopolitical player with one of the world's largest nuclear complexes? Politically, Russia is likely to zigzag between expanded democratic institutions and a more vigorous civil society, on the one hand, and an authoritarian regime managed by security-service professionals under formal democratic procedures, on the other. In either case, it would be heartening to know that, should security culture take root in Russia, nuclear materials would be less likely to fall into the hands of those intent on doing Russia–and the West–harm. ■

APPENDIX I

CASE STUDIES

The two case studies below were developed to illustrate the point that a group of unscrupulous employees, including managers and lower-ranking operators acting in collusion, can effectively divert and steal valuable materials from their workplace despite seemingly airtight security and anti-theft precautions. A good security culture could have prevented such acts, or at least made them much more difficult to carry out. One case describes the criminal operation at Elektrokhimpribor, a top-secret nuclear weapons facility in the closed city of Lesnoy. The other took place at a major gold-refining plant near the small town of Kasimov, not far from Moscow.

CASE STUDY I

Isotope Diversion at Elektrokhimpribor Facility

A major scandal related to nuclear facilities in Russia took place in the early 1990s at the Elektrokhimpribor Facility, a top-secret nuclear-weapons plant in the closed city of Lesnoy. It involved the theft of a large amount of rare and expensive isotopes. The case involved not only employees from all levels at the facility, ranging from workers to top management, but also senior officials from the Ministry of Atomic Energy (Minatom).

Russia accounted for up to 80 percent of the world market in stable isotopes by the 1990s. Only three facilities in Russia produced the isotopes sold abroad: the Electrochemical Instrument Building Combine (Elektrokhimpribor), which produced 80 percent of the country's total, the Electrochemical Facility in Krasnoyarsk, which accounted for some 15-18 percent of production, and the Kurchatov Institute, which made up the remaining 2-5 percent. The key Russian competitor on the export market was the Oak Ridge National Laboratory in the United States, while China ranked third among producers of stable isotopes. After the collapse of the Soviet Union, Russian companies tried to export isotopes on their own, but the increase in supply due to their efforts drove down prices on the world market. Russian isotope exports dropped dramatically with the slide in prices. In 1992 the Russian government established an export company, Stabis Ltd, to structure, centralize, and improve Russian isotope exports. Stabis was headed by Alexander Podkidyshev.

The Elektrokhimpribor Combine is located in the closed city of Lesnoy, formerly known as Sverdlovsk-45. The plant was responsible for assembling, and later dismantling and storing, nuclear warheads. Construction of Elektrokhimpribor began in 1947 with Plant 418, which initially produced highly enriched uranium (HEU) using an electromagnetic separation technique. In the late 1950s the separation facility was redirected to produce stable isotopes of elements such as thallium, rubidium, zinc, and other non-uranium elements, while a portion of the plant was used to house a warhead assembly/disassembly facility.

As a closed city, Lesnoy did not exist on the map before the end of Cold War. Access is still restricted to holders of a special pass. Elektrokhimpribor remains the key facility in town. Its employees were highly paid during the Cold War and did not experience any financial problems. The collapse of the Soviet Union, however, hurt them, as it did employees elsewhere in the nuclear industry. Inefficient management and marketing, products of the Soviet-era economy, hampered

efforts to export isotopes efficiently. Far away from the big cities and tied to jobs at their facility, managers at Elektrokhimpribor tried to find a way to improve their financial situation. Stable isotopes are rare and expensive goods used in different industries; the facility managers knew the price their product could command and tried to sell it on their own.

The scheme was so well managed that the fact of diversion became known only by a fluke. The conspirators did not bother to hide their expensive cars and houses, which were incongruous in a very small town where the main industry, Elektrokhimpribor, paid small salaries. This incongruity attracted the attention of law-enforcement officers who drew a parallel between the financial well-being of several employees at the facility and the situation on the very small world market in isotopes, where prices had dropped dramatically and it had become surprisingly hard to sell anything. Initial accounting audits at the facility, however, provided few leads.

The investigation ultimately revealed that the members of the group had used their positions to produce "unaccounted for" isotopes beyond officially reported production. Because the conspirators worked at each stage of production, they were able to establish a parallel isotope production process–producing isotopes identical to those turned out by the plant during normal operations.

The core of the conspiracy included nine employees of Elektrokhimpribor: Kascheyev, director of the production of stable isotopes; Yaroslavtsev, his deputy; Tunin, the head of the technical section; Tuinov, an engineer; Konoplina, the head of the chemical production department; Usoltsev, her assistant; Dubinin, a specialist in finished chemical production; Chernousov, a specialist in chemical apparatus and production; and Korolev, the deputy head of the financial department of the combine. They diverted stable isotopes such as thallium-203, zinc-68, rubidium-87, ytterbium-168, and tantalum from the plant.

The scheme was devised by Kascheyev, an academician and inventor who claimed that, because he had used waste materials and an isotope purification technique he had invented, the activities of the group were perfectly legal. He also pointed to the fact that the isotopes had been exported through a legitimate federal isotope-exporting company.

The conspirators were skimming off 5-10 percent of the enriched isotope solution they were using in the production process, and then diluting the solution with distilled water to avoid detection. The diverted solution was accumulated separately, then processed using experimental units which were being tested at the facility. The illegally produced isotopes were sealed in tubes and removed from the facility without detection. At first, the group had difficulty finding customers or middlemen for the material. Then they established a stable distribution channel through Stabis Ltd., a Moscow-based private company. The director of Stabis, Alexander Podkidyshev, who was also head of the Russian State Center for Stable Isotopes, purchased the illegal isotopes at below-market prices, then resold them to his own company at a large profit. Most of the isotopes, which are used for medical and industrial purposes, were then exported from Russia.

The investigation and trial took several years. In May 2000 a federal court found all members of the group guilty in accordance with Article 160 of the Criminal Code. (Titled "Misappropriation and Peculation of Federal Property," Article 160 prescribes jail sentences ranging up to three years for such offenses. Those found guilty of repeated acts of misappropriation, as well as individuals who abuse official authority in the commission of a crime, are subject to prison terms ranging up to six years.) The court sentenced them to three years' imprisonment without seizure of property, but it freed them because they had already been in custody for over three years by the time the sentence was handed down, and because of an amnesty granted them. All of the participants in the isotope case except for the head of Stabis, Alexander Podkidyshev, were released following the verdict. Podkidyshev received an additional two-year jail term. The convicted thieves resumed work at the site, although their security clearance status was reduced and they could not return to

their previous positions of authority. The government rewarded the enforcement officers who had cracked the case.

Much has changed in Russia since that incident. Even so, the case illustrates several enduring themes about the Russian nuclear sector:

- It is a simple matter to steal or divert strategic materials from a Russian nuclear facility when workers and managers are complicit in the theft or diversion. The conspiracy at Elektrokhimpribor was discovered by a fluke; otherwise it could have kept going indefinitely.
- A culture of obedience to the law is not common in Russia, where the public tends to excuse illegal actions as "a way out of poverty." The participants in the Elektrokhimpribor proliferation ring denied that they had done anything wrong. Their colleagues who had not been involved in illegal activities justified the conspirators' actions by claiming that "there was no other way for people to make money." Whistle-blowing practices do not work in Russia; thus nobody reported the crime.
- The law is not rigidly enforced. Participants in the "isotope affair" received no punishment apart from the time served awaiting trial. Their property was not seized, and they even returned to work at the same closed facility, albeit without the security clearances they had formerly enjoyed.
- Despite this well-publicized case, the security situation at Lesnoy did not improve noticeably. Several incidents were reported. In November 2000, for instance, a soldier on duty at the Elektrokhimpribor Combine opened fire on his fellow soldiers before committing suicide. In March 2002, three armed Chechen nationals were detained in the Sverdlovsk region, one of whom had a pass to the closed city. In August 2002 a conscript soldier, Denis Bragin, deserted the military unit assigned to guard Lesnoy. Bragin wounded a fellow soldier with a knife when the latter attempted to stop him, and he fled the unit with an AK-74 Kalashnikov rifle and the associated ammunition. Media reports indicated that Bragin should not have been entrusted with a weapon in any event, as he had a history of psychological problems. □

CASE STUDY II

CORRUPTION AND THEFT AT PRIOKSKIY GOLD REFINING FACTORY

Another case involving massive corruption, racketeering, conspiracy, and collusion among responsible personnel took place at Priokskiy, a gold refining plant near the small town of Kasimov, not far from Moscow. The case illustrates just how vulnerable are sensitive industries in Russia to corruption and criminal infiltration, and it underscored how important it is to establish and nurture a culture of security among those entrusted with sensitive goods and technology–from the top down.

During the years of steady economic decline, especially in the late 1980s, the Soviet Union had managed to deplete its strategic gold reserves to almost nothing. Given the weakness of the national economy, gold was seen as a way to generate much-needed hard cash and to provide a foundation for making the ruble a freely convertible currency. In 1989, the Soviet government decided to build a new gold refining factory in the town of Kasimov, in Ryazan oblast. The new factory would produce gold bullion of higher quantity and purity than the three existing facilities: Its total annual output was 500-600 tons of 99.99 percent refined gold and 2,000 tons of silver. The factory was built from scratch in 18 months and received the most elaborate security system available at the time.

The first warning signs came in 1992, when a string of strange and seemingly unrelated murders and disappearances involving local businessmen, visitors, unemployed citizens, and some factory personnel took place. Investigators suspected that these events might be connected to illegal activity at the gold refining factory and ordered a surprise inspection. They discovered, however, that not a single milligram of gold was missing.

The next warning bell rang in 1994, when two individuals were detained in Nizhny Novgorod after asking a grocery shop attendant to weigh a kilogram of industrial gold bullion. During the ensuing investigation, the two admitted to acquiring the gold through a chain of accomplices from someone who was working at the Kasimov factory. Moreover, both admitted to having previously sold 22kg of gold from the same source. The gold had apparently originated from the factory, despite the fact that the inspectors had been unable to find a single missing milligram. Due to the large volume of material stolen, a special, high-level investigating team was appointed, and a new, more thorough inspection and accounting was carried out at the factory. But again, not a single missing milligram of gold was uncovered.

Over the next few months the factory's security system was reevaluated and rechecked. The system consists of two security perimeters: An internal Perimeter B includes the main production line and is surrounded by two rows of barbed wire, a sand strip for intruder detection, and a system of security cameras and motion detectors. Perimeter A on the outside includes auxiliary services and access to the city. To get from Perimeter B to Perimeter A, an employee had to go through a "nude zone," where all employees had to be strip-searched. None of the components of this security system seemed at the time to have been compromised.

Realizing that the missing gold must have come from somewhere, the investigators kept searching for a drop spot, and after some days discovered a workman's glove that contained a large piece of gold bullion. After further investigation, a group of employees from the same shift admitted to taking 78kg of gold and hiding it in various locations within the facility. They all maintained, however, that they had not carried the gold out of the factory. Although they admitted to having been paid for the drops, none of the employees would reveal the source of the payments. In the course of the interrogations, investigators came up with the following findings:

- Large quantities of gold continued to be diverted from the factory despite the arrest of the group.
- Organized criminal groups must have played a large role in the scheme. This would explain the refusal of the arrested employees to reveal who had paid them to purloin the gold, not to mention the continued string of assassinations and murders.
- Some security personnel at the factory must have been involved, because it was not possible to bypass the security perimeter without their knowledge.
- Finally, there was no explanation for the fact that the factory accounting system failed to identify any loss.

In early 1995, intelligence was received indicating that large quantities of illegal gold bullion had appeared on the black markets in several former Soviet republics and Turkey. Investigators began a massive search for drop spots and hiding places throughout the facility, uncovering numerous locations and apprehending several employees, who revealed the means by which gold had been spirited out of the secure zone. Despite common knowledge among the workforce about these 24-hour spot searches and raids, a large volume of gold continued to be stolen, including even a standard gold bar used for weighing and measurement. One trick involved literally shooting gold outside the perimeter: During one of the raids, investigators discovered an axe used to hew gold bullion bars into smaller pieces and a slingshot used to shoot the fragments out. The pieces were retrieved later. Another trick involved cutting open sewer pipes, allowing packets of gold to be transported outside. And walls were broken through to the outside, repaired, and then broken again to allow small packets to be thrown outside the compound.

Investigators managed to uncover other pieces of the puzzle. First, they suspected and subsequently confirmed that a head of the security guard detachment at the perimeter access point was part of a group of security personnel who themselves had carried, or allowed others to carry, large quantities of gold. During security checks, these security officers would manually turn off the metal detectors used to scan each employee leaving the security perimeter, and pretend that they had performed the checks.

Second, it finally became clear how the plant had managed to produce the same quantity and quality of gold despite massive theft. During the refining process and electrolysis, a local engineer, showing remarkable ingenuity, had found a way to add extra quantities of copper to the process which did not affect the final product. His nickname was Academician. The engineer was identified by the investigators, arrested, interrogated, and then released. Several days later he was found dead in his car, apparently murdered for disclosing information about the scheme.

When finally the whole picture of the conspiracy was revealed, it turned out that virtually everybody at the plant was involved, ranging from operations personnel to security guards to management, and that an outside network of distributors was involved as well. Among those caught were the coach of the factory soccer team, the deputy director and head of a specially appointed internal investigation team, and a head of the security guard, who held the rank of major and, on one occasion, had personally carried 30kg of gold two miles outside of the perimeter.[1]

Overall, a total of 400kg of gold was found to have been stolen, and another 210kg was later recovered. Fifty-two people were murdered as part of internal fighting within the organized criminal groups. One hundred twenty-eight facility employees were convicted of various felonies; 30 security

1. "Heavy Gold of Kasimov," *Market of Precious Metals and Precious Stones Newsletter*, May 16, 2003, <http://www.rdmk.ru/info/news/lenta/2003_05_16_08_05>.

personnel, all officers of the Ministry of the Interior hired with best recommendations to guard the facility, were convicted and sentenced to time in prison for their participation in the scheme.[2] Since 1997, when the cases were closed, no organized criminal activity has been reported in the area, and no gold has been found missing. ■

2. For more information, see "Gold-Diggers," *Sovershenno Sekretno* 4 (2000), <http://www.sovsekretno.ru/2000/04/11.html>.

APPENDIX II

LEARNING AND PROFESSIONAL IMPROVEMENT: A METHODOLOGY FOR SECURITY CULTURE IN RUSSIA

The main element of the Security Culture Mechanism designed to operate inside the nuclear facilities is the performance of leadership. Top managers (director and deputy directors of the site) are responsible for initiating, developing, and implementing a specific set of policies and procedures to shape the behavior of their subordinates. Continuous training is the primary tool to get the required results. While in Western societies leaders rely primarily on legal norms and time-tested management practices in the course of their daily work, leaders in transitional countries like Russia enjoy more legal leeway and can do much more at their own discretion. Thus, site leadership in Russia is critically important to the process of improving or degrading nuclear security culture. Training of top managers is intended to reinforce their assumption of vulnerability as a prerequisite for introducing a healthy security culture (see Figure 1), as well as to equip them with state-of-the-art managerial tools to implement this culture in practical terms.

The training curriculum for top managers would include three modules and a workshop (see below). The applicability of each module depends on the mission of a specific facility, risk assessment, and the time which can be allocated to training. It should be compatible with the educational background, experience, knowledge and skills, and goals of the trainees. Modules would include a security threat assessment block, a block covering the main components of security systems and the operations of these systems, and a personnel management block.

Training of top managers should be followed by training of other site employees, specifically tailored to the needs of each level of the organizational hierarchy. Other target groups include:

- Mid-level managers (heads of shops, offices, laboratories, etc.)
- Reserve top managers
- Technical specialists/experts
- Other personnel who have access to nuclear material
- Guards (departmental, interior troops, military, escorts)
- Outside inspectors
- Experts in psychological and medical science

The training modules for these groups would consist of the following:

- *Initial Training*. New employees should receive baseline instruction on policies, issues, and incident response/reporting procedures. The training should be tailored to an individual's job within the facility and short enough to be easily comprehensible. Accession training can range from classroom instruction to computer-driven self-study modules. New employees should be

quizzed briefly to assure that they grasp the essential elements of the training, and they should be required to sign a statement certifying that they understand its content.

- *Periodic Training*. The essential elements from the initial training should be reviewed regularly. Additionally, special sessions should be held when policies and procedures are updated. Attendees should be quizzed again to assure comprehension, and required to sign a new statement verifying their attendance. Training can be performed annually, quarterly, or as needed.

- *Ongoing Programs*. Ongoing programs are one of the most effective tools available to the security-aware facility. They include traditional methods such as wall posters, handouts, and memos, as well as more interactive methods such as monthly email updates and special bulletins reviewing the lessons-learned from internal and external security incidents.

- *Ongoing Assessment*. This will vary highly depending on the resources available to the facility and its actual security needs. Still, management should conduct appropriate and random assessments to ensure the training is effective. Top managers should drop in on training sessions unannounced.

- *Quality Assurance on Training and Trainers*. It is important to get feedback on the training programs and materials, as well as the trainers themselves. Those responsible for training should include quality assessment as part of the program. Feedback should be solicited from those who undergo the training, in the form of post-training evaluations. The insights gleaned from this process should be used to refine the training curriculum.

CURRICULUM OUTLINE FOR TOP MANAGERS

I. Nuclear Security Threat Assessment

This block would be of particular importance to those sites which are not currently involved in international nonproliferation training programs, and thus are less aware of nonproliferation threats and international practices.

1. Nuclear Security Threat Assessment

This section would introduce nuclear managers to the basics of nonproliferation, improving their awareness and helping them understand why nuclear security awareness is important. It would include such lectures as:

- Threat assessment. Types of threats, detection and response, introduction to Design Basis Threat (DBT) analysis
- Terrorism involving weapons of mass destruction. Terrorism threat assessment
- Importance of nonproliferation and security awareness. Case studies involving smuggling and diversions. Best security awareness practices
- Security Culture Mechanism and ways to develop a security culture (Security culture development is discussed below, throughout the training session.)

2. Nuclear Materials Management in Russia and International Practices

The section would cover general Russian and international practices and approaches to nuclear materials storage, disposition, transactions, packaging, transportation, and consolidation. It would also cover material protection, control, and accounting (MPC&A), including reporting requirements and data submission, safeguards, information protection, and waste management. International approaches and practices pertaining to the development and improvement of nuclear security awareness and nuclear security culture would also be reviewed.

3. Cooperation on Nuclear Security

This section would provide an overview of U.S.-Russian bilateral programs and G-8 programs, covering the origins of these programs, subsequent developments, changes in the programs' scope, positive and negative case studies, future possibilities for development, and ways to improve sustainability.

II. Material Protection Control and Accounting

The block would provide insight into the workings of security systems, outline the main components of these systems, explain how these components operate together, and review their main functions and goals. This block would be of particular importance for those managers who do not have a technical background in nuclear security. It would help them recognize and solve problems.

1. Fundamentals of Material Protection Control and Accounting

The main focus of this block would be to explain why MPC&A is important. It would go into greater detail than did the first block, providing more in-depth knowledge about security systems and ways to improve them. It would cover the following elements:

- MPC&A as an integrated system. Elements of MPC&A
- *Nuclear Materials Control:* administrative controls, access controls, surveillance, containment, and detection/assessment mechanisms
- *Nuclear Materials Accountability*: generally accepted accounting principles, accounting systems, physical inventories, inventory difference control limits, measurements and measurement control, and reporting
- *Nuclear Materials Physical Protection*: threat definition, target identification, sensors and alarms, response forces, analysis and evaluation techniques, and transportation of nuclear materials
- *Site and Personnel Security:* operations security
- Evaluating the effectiveness of MPC&A programs

2. International Approach to MPC&A: Integrated Safeguards and Security Management

This section would describe a systematic approach to integrating safeguards and security into different states' practices. It would provide a detailed overview of policies and practices used by the United States and the International Atomic Energy Agency (IAEA) to establish, develop, and improve nuclear security awareness and nuclear security culture.

3. The Methodology of Risk Assessment

This section would compare and contrast the Russian, IAEA, and Western approaches to this important topic and build a viable model for Russian sites to use. It would include: fundamental concepts of DBT; an introduction to vulnerability analysis (VA), including threat assessment, risk management, response design, and the evolution of these factors in a changing environment; basic VA terminology and concepts, and the mechanics of conducting VA; threat and target characterization; differentiation between internal and external threats; security and surveillance system characterization; scenario development; system effectiveness evaluation; and upgrade identification and prioritization.

4. Legislative and Regulatory Framework for Russian Nuclear Security

Instructors would apprise nuclear facility managers about the basics and continuously changing legal and regulatory environment associated with nuclear security. Both the Russian national regulatory framework (federal, industry, site) and Russia's obligations under the multilateral nonproliferation mechanisms would be examined. The instructors would also discuss the Federal Information System, the impact of the general-scope legal basis and the regional legal basis for security precautions, and ways to improve the legal basis.

5. Nuclear Materials Management Liability, Liability for Nuclear Security Norms Violations, and Enforcement

Instructors would examine nuclear materials management and operations, the general-scope and security-specific legal bases, and criminal and administrative liability for mishandling nuclear materials and violating regulations. Case studies would be discussed.

6. Introduction to Information Security and Cyber Security Awareness

The section would cover policies and procedures for control of classified information, Internet access, and electronic data transfers. Access tracking systems and communication control would also be addressed. Trainees would be provided with an introduction to briefing systems.

7. Emergency Operations and Accident Response

Along with operations under emergency conditions and in case of accidents, this section would cover crisis prevention, management, and negotiation. Instructors would also go through case studies, discussing industry-wide accident databases and mechanisms for learning from experience.

III. Personnel Management

1. Personnel Management at Nuclear Facilities: Russian and International Experience

The course would include, among other things:

- Personnel management rules, regulations, manuals, and practices
- Strategic and tactical decisionmaking, policymaking, and methods of balancing priorities. Proactive policies and procedures
- Best leadership practices and tools for establishing effective leadership

- Position and job classification, personal responsibilities, recruitment, and termination
- Performance assessment, testing, and control. Work measurement
- Personnel reliability control and screening. Quality control
- Personnel motivation. Encouraging teamwork and collaboration
- Personnel training and retraining
- Change management
- Psychological management, including conflict resolution and techniques for establishing an organizational culture and motivating personnel
- Contingency plans and drills
- Operations under emergency conditions
- Information control

2. Introduction to Industrial Psychology and Testing for Nuclear Industry

This section would offer nuclear facility managers more detailed information about the tools necessary to evaluate the psychological and emotional fitness of prospective employees during the recruitment process and periodically throughout their employment. It would also present a methodology and practices for conflict resolution, as well as procedures for mental and psychological evaluation, personnel reliability control, screening, and medical and drug tests.

3. Performance Assessment and Improvement

This section would introduce trainees to methods for work measurement; performance testing (e.g., equipment, procedures, and personnel); establishment of benchmarks for worker performance; peer-assessment and self-assessment; development and enforcement of codes of conduct; quality control; development of teamwork in the workforce; investigation and analysis of anomalous conditions; and the process of corrective action.

4. Organizational Culture

This section would present both theoretical and practical approaches to forming an organizational culture conducive to high standards of security culture among the personnel at nuclear facilities. It would introduce mechanisms and techniques for developing personal responsibility and accountability, involving personnel in the improvement process, soliciting and using feedback, and improving communication lines. Instructors would present best international and Russian practices and approaches, both in the nuclear sector and in other private and public industries, and discuss best leadership and management practices used to establish a thriving organizational culture.

5. Incentives and Motivation for Nuclear Security Personnel

This section would cover the use of positive and negative incentives, recruitment, performance evaluation, open communications, the use of authority, supervisory techniques, non-monetary incentives, and other forms of motivation. It would combine Western theories and practices of personnel management with the realities of the Russian corporate and industrial culture and work ethics.

6. Job Classification for Nuclear Personnel

This section would offer nuclear facility directors the skills needed to tailor job descriptions for employees at critical facilities, ensuring that these personnel are fully familiar with their duties and responsibilities and that they are properly compensated. Instructors would outline the skills and mechanisms necessary to write and efficiently manage instructions. They would also outline required procedures pertaining to job classification and discuss recruitment and termination processes and requirements.

7. Personnel Training

This section would assist managers in their effort to establish on-site training courses and programs in security culture for all types of personnel. Of particular interest are training for inspectors, "train the trainer" programs, techniques for developing courses and manuals, methods for writing instructions, and personnel supervision. Instructors would discuss procedures and practices for initial training, periodic training, and ongoing training; briefings, contingency plans, and drills; and training standards and expectations. They would share techniques for assessing the performance of trainees and trainers. Quality assurance and best practices would be examined.

8. Introduction to Marketing and PR

One part of this section would be intended to help managers market their facilities' products more efficiently. Since each facility is responsible for paying for security upgrades, it has to be financially sustainable to support these upgrades, keep qualified employees at the facility, and motivate employees to work efficiently and comply with security norms. Another part would introduce managers to the basics of PR and public outreach, helping them improve public awareness and, in turn, solicit the help of the public in improving security. Reducing misunderstandings and conflict over environmental and other issues would be an added benefit. Western experience, policies, and practices for improving public awareness would be widely used.

IV. Workshop/ Roundtable Discussion

Managers would discuss and share their experiences, focusing on how they view the strategy and tactics of developing and implementing security culture. Typical seed questions would be, "What are the most critical and most challenging areas of developing and implementing a security culture?" "To what extent does the security culture exist and to what extent it is being implemented at individual facilities?" and "What can be done to improve security culture standards?" ■

APPENDIX III

NUCLEAR SECURITY CULTURE EVALUATION

This questionnaire represents the first iteration of a comprehensive evaluation methodology designed to help nuclear industry management gauge the existing security culture among the management and employees of nuclear facilities. The questions are designed to capture both the tangible aspects of security culture and the working environment, such as procedures, rules, and regulations, and intangibles such as behavior, attitudes, and the prevailing mentality among the workforce. The questionnaires will be administered anonymously to elicit the most candid feedback possible from respondents.

The questionnaire includes questions that ask respondents to evaluate elements of the security culture on a scale from 1 (not applicable/nonexistent) to 5 (excellent/fully existent/fully complied with). (2 – in bad shape, poor; 3 – satisfactory; 4 – good). This quantitative methodology will allow users not only to assess the condition of security culture within a given organization, but to compare security cultures from facility to facility. An index of security culture effectiveness, derived from a weighted average of the scores, will make a useful benchmark for comparison.

The index evaluates the security culture in four categories: (1) Leadership, (2) Policies and Procedures, (3) Learning and Professional Development, and (4) Personnel Performance. Each category has a maximum score of 5. An ideal security culture, then, would earn a perfect score of 20, or 100 percent.

Each category is broken down into elements (A, B, C, etc.). The elements are further broken down into individual questions (1, 2, 3, etc.). The score for each element comes from averaging the responses to individual questions, and the score for each category is totaled up by averaging the scores for the constituent elements.

The elements will vary in relative importance from country to country. Each element, accordingly, will be weighted numerically according to its relative importance. In one country, efforts of management to set standards might be more important than open communication within the workforce. The opposite could be true in another country. The relative weights assigned to different features in a particular nuclear security culture will be established by surveying a sizable group of experts in a given country. Respondents will be asked to weight each element based on its importance, using a 100 percent scale, and to define a minimally acceptable score for each element.

This survey lays out the questions by thematic category. The questionnaire is generic to all categories of operational personnel. Further refinement of the methodology will yield questionnaires tailored to different audiences, such as industry management, facility leadership/management, and operations personnel.

Appendix III breaks down the categories of respondents for whom the methodology will be tailored. Security culture can be evaluated at given facilities or groups of facilities in a particular country, allowing researchers to, say, detect cultural variations from region to region or facility to facility.

I. Leadership

(Unless otherwise noted, please answer the following questions on a scale from 1 (not applicable/nonexistent) to 5 (excellent/fully existent/fully complied with).)

A. Standards and expectations

1. To what extent does the facility management set clear standards and expectations for personnel in the security area?
2. How aggressive has the facility management been in promulgating
    a. sets of rules and regulations?
    b. guidelines, manuals, or instructions?
    c. specific, security-related items in the organizational charter/mission?
3. To what extent does the facility management promote an organizational culture focused on continuous improvements to security?

B. Decisionmaking

1. To what extent does the facility have strategic and operational plans in place to improve security?
2. To what extent does management work to improve security at the facility?
3. As far as you know, do top managers themselves always follow established security procedures and directives?
4. How frequently/regularly does the facility management conduct the following for individual personnel? (Rate each activity from 1 (not at all) to 5 (regularly in accordance with established policy).)
    a. planning?
    b. setting performance benchmarks?
    c. assigning responsibilities?
    d. monitoring?
    e. rating performance?
    f. rewarding good performance and punishing substandard performance?

C. Use of authority

1. To what extent does the facility management use its authority effectively to achieve strategic and operational goals?
2. To what extent is the facility management aware of security-related problems and needs?
3. To what extent does the facility management use training to encourage security awareness among employees of the site?
4. To what extent does the facility management offer
    a. monetary and non-monetary performance incentives?
    b. other forms of employee motivation?
5. To what extent does the facility management offer conflict resolution?

D. Supervision

1. How effectively does the facility management supervise employees?
2. Does the facility have in place written policies, rules, or procedures for recruitment, appraisal, and termination of employees as they pertain to security?
3. To what extent does management encourage and/or enforce
    a. teamwork?
    b. personal responsibility/accountability for security improvements?

E. Involvement of staff

1. Are employees sufficiently involved in the decisionmaking process?
2. To what extent are employees involved in developing instructions, rules, and regulations?
3. To what extent does the facility management
    a. require/request feedback from employees?
    b. seek recommendations and suggestions relating to security improvements?

F. Open communication

1. Do managers make themselves readily available to employees to discuss questions, procedures, or concerns regarding security improvements? It there an open-door policy?
2. To what extent does the facility management encourage employees to report problems, security breaches, violations of instructions, failures by management, hazardous conditions, and other security-related problems?
3. Do rank-and-file employees at your facility consider themselves valuable members of the organization? Do they believe management values their contributions?

G. Improving performance

1. To what extent is the facility management committed to improving employee performance?
2. How regularly does the facility management conduct performance evaluations? (From 1 (not applicable/nonexistent) to 5 (regularly in accordance with established policy))
3. How regularly does the facility management discuss accidents and derive lessons-learned in order to prevent similar events from happening in the future? (From 1 (not applicable/nonexistent) to 5 (regularly in accordance with established policy))

II. Policies and Procedures

(Unless otherwise noted, please answer the following questions on a scale from 1 (not applicable/nonexistent) to 5 (excellent/fully existent/fully complied with).)

A. Visibility of security policies

1. Are security procedures posted in the workplace? If not, has management made other efforts to apprise employees of their security-related responsibilities?
2. How effectively does management communicate information about security policies to the workforce?
3. To what extent is the facility's accident database available to facility employees for their use and review?
4. To what extent is the industry-wide accident database available to facility employees for their use and review?

B. Employee code of conduct

1. Has your facility instituted an employee code of conduct?
2. To what extent are security-related duties included in the code of conduct?
3. How familiar are employees with the code of conduct?
4. How regularly are employees briefed on, and required to know, the code of conduct? (From 1 (not applicable/nonexistent) to 5 (regularly in accordance with established policy))

C. Roles and responsibilities

1. To what extent does your facility have special procedures for developing employee job descriptions and position requirements?
2. To what extent does your facility have position requirements?
3. To what extent are job descriptions in line with position requirements?
4. To what extent are responsibilities assigned to employees by the managers in line with position requirements and job descriptions?

D. Performance measurement

1. To what extent does your facility have special performance measurement procedures?
2. To what extent is security-related performance a part of overall performance assessment?
3. To what extent does performance assessment include
    a. team/group performance assessment?
    b. self-assessment?
    c. individual peer-assessment?
4. To what extent is satisfactory performance in security-related duties a prerequisite for continued employment?

E. Work environment

1. To what extent does the facility management provide and encourage a positive work environment?
2. To what extent are employees satisfied with their work environment?
3. To what extent does the facility management provide the resources necessary to improve security?
4. Is equipment maintenance conducted on time? (From 1 (not applicable/nonexistent) to 5 (regularly in accordance with established policy))

F. Work measurement

1. To what extent does the facility management follow and enforce strategic and operational plans?
2. To what extent does the facility management effectively control employees?
3. To what extent does your facility have adequate recruitment and training procedures?
4. Would a person be laid off/terminated in case of failure to follow security regulations?

G. Information control

1. To what extent does the facility have specific rules on handling security information?
2. To what extent does the facility enforce information control policies?
3. To what extent are these rules followed by employees?
4. How regularly does the facility management offer briefs on handling classified information? (From 1 (not applicable/nonexistent) to 5 (regularly in accordance with established policy))

H. Material accounting system

1. To what extent does your facility have a modern material accounting system?
2. How adequate are special nuclear materials access/equipment operation procedures?
3. How effectively have these procedures been implemented?
4. As far as you know, how regularly are material accounting audits taken? (From 1 (not applicable/nonexistent) to 5 (regularly in accordance with established policy))
5. To what extent have material control and accounting (MC&A) reporting procedures been instituted at your facility?
6. To what extent does the facility comply with MC&A reporting procedures?
7. To the best of your knowledge, is your facility's procedure for reporting a loss of material adequate?

I. Cyber protection

1. Is your facility adequately protected from cyber attack?
2. How effectively is Internet use controlled and restricted?
3. To the best of your knowledge, how effective are your facility's precautions against transfers of sensitive information
    a. outside of the facility?
    b. within the facility?

J. Employee screening

1. Are employees adequately screened by the security service prior to starting work at your facility?
2. To the best of your knowledge, to what extent is the screening procedure compatible with the requirements for a particular position?
3. To the best of your knowledge, are the following conducted at your facility? (From 1 (not applicable/nonexistent) to 5 (regularly in accordance with established policy))
    a. background checks?
    b. medical screening?
    c. psychological screening?
    d. drug screening?
    e. alcohol screening?

K. Quality control

1. To what extent does the facility have effective product/process quality control measures?
2. Are these measures adequately enforced?
3. To what extent do quality control measures include security improvements?
4. To what extent do quality control measures include
    a. process mapping and visualization?
    b. process control and audit?
    c. process improvement?
    d. integration of people, process, and technology?

L. Change management

1. To what extent does change at your facility influence security?
2. To the best of your knowledge, does management have the special capabilities/practices needed to manage change without negatively affecting security?
3. To what extent does management encourage initiative and innovation, particularly with respect to improvements in security?
4. To what extent is management resistant to change?

M. Operating experience feedback

1. To what extent are management and operating personnel aware of externally imposed performance benchmarks and other facilities' experiences with improving security?
2. How regularly are accidents at your or other facilities analyzed and discussed in order to prevent similar events from happening in the future? (From 1 (not applicable/nonexistent) to 5 (regularly in accordance with established policy))

III. Learning and Professional Improvement

(Unless otherwise noted, please answer the following questions on a scale from 1 (not applicable/nonexistent) to 5 (excellent/fully existent/fully complied with).)

A. Initial training

1. To what extent does the facility have a developed employee training plan?
2. Do employees undergo initial training at the start of their tenure at the facility? (From 1 (not applicable/nonexistent) to 5 (regularly in accordance with established policy))
3. Is there an employee security briefing system at your facility? (From 1 (not applicable/nonexistent) to 5 (regularly in accordance with established policy))
4. Specifically, how regularly does the facility conduct
    a. initial briefings?
    b. comprehensive briefings?
    c. refresher briefings?
    d. termination briefings?

B. Periodic training

1. How regularly do employees undergo periodic training during their tenure? (From 1 (not applicable/nonexistent) to 5 (regularly in accordance with established policy))
2. How well developed is the on-site training system?
3. How regularly does the facility send employees to central locations/institutes for continued professional training? (From 1 (not applicable/nonexistent) to 5 (regularly in accordance with established policy))
4. Does the facility have its own trainers?

C. Ongoing training

1. To what extent does the training provided at/by the facility address employee/facility needs?
2. To what extent does the facility have training manuals, guidelines, or handbooks?
3. To what extent does the facility have "train the trainer" programs?
4. Are adequate training facilities and materials available?

D. Ongoing assessment

1. Are employees assessed periodically on their knowledge and skills? (From 1 (not applicable/nonexistent) to 5 (regularly in accordance with established policy))
2. To what extent are special training assessment procedures and techniques available?
3. To what extent does the facility management measure the effect of training on employee job behavior?
4. To what extent does training contribute to improvements in worker attitudes and security awareness?

E. Quality assurance on training and trainers

1. To what extent does the facility exercise quality control over the training subject matter and the trainers themselves?
2. How regularly does management disseminate special surveys and questionnaires to assess the quality of training and trainers? (From 1 (not applicable/nonexistent) to 5 (regularly in accordance with established policy))
3. To what extent is this feedback taken into account when future training sessions are planned?

F. Contingency plans and drills

1. To what extent does the facility have contingency plans and drills?
2. Are these contingency plans updated regularly? (From 1 (not applicable/nonexistent) to 5 (regularly in accordance with established policy))
3. To what extent are these plans and drills adequate to the security threat?
4. How regularly does the facility conduct drills? (From 1 (not applicable/nonexistent) to 5 (regularly in accordance with established policy))
5. To what extent does the facility cooperate with rescue teams, emergency management agencies, and other response personnel?

IV. Personnel Performance

(Unless otherwise noted, please answer the following questions on a scale from 1 (not applicable/nonexistent) to 5 (excellent/fully existent/fully complied with).)

A. Professional conduct

1. To what extent do employees, generally speaking, consider their work valuable and prestigious?
2. To what extent do you personally consider your work valuable and prestigious?
3. To what extent do employees consider themselves personally responsible for security at the facility?
4. To what extent do you consider yourself personally responsible for security at the facility?

B. Personal responsibility/accountability

1. To what extent do employees know their job responsibilities and assignments?
2. To what extent do employees know the security norms, rules, and procedures relevant to them?
3. To what extent are the roles and responsibilities of employees clearly defined in their job descriptions?
4. How often are employees requested to perform work they are not qualified to do? (From 1 (not applicable/nonexistent) to 5 (regularly in accordance with established policy))

C. Following procedures

1. To what extent does the facility have developed instructions, procedures, policies, and normative documents related to security?
2. Are the facility's instructions on security clear, relevant, up-to-date, user-friendly, and results-oriented?
3. Do employees usually follow procedures and instructions? (From 1 (not applicable/nonexistent) to 5 (regularly in accordance with established policy))
4. To what extent do visible enforcement measures exist at the facility to encourage employees to follow procedures?

D. Teamwork and collaboration

1. To what extent are employees encouraged to work as a team?
2. To what extent are the roles and responsibilities of team members clearly defined?
3. Are there restrictions in place to prevent employees from performing functions not officially assigned to them?
4. How regularly is cross-training conducted? (From 1 (not applicable/nonexistent) to 5 (regularly in accordance with established policy))

E. Whistle-blowing procedures

1. To what extent are employees encouraged to question suspicious activities and report on such to their supervisors?
2. To what extent are special reporting procedures in place? Does the facility have a hotline and/or a specific person in charge of these procedures?
3. To what extent are anonymity and job security guaranteed to a person who reports security problems?
4. To what extent do employees know the reporting procedures? Do they know whom to notify about security problems?

NOTES

NOTES

Center for International Trade and Security
120 Holmes/Hunter Academic Building
University of Georgia
Athens, GA 30602