Safeguarding Nuclear Weapon-Usable Materials in Russia

by
Thomas B. Cochran

Presented
at the
International Forum

Illegal Nuclear Traffic: Risks,
Safeguards and Countermeasures

12-13 June 1997

Como, Italy

NATURAL RESOURCES DEFENSE COUNCIL, INC
1200 New York Avenue, N.W., Suite 400
Washington D.C. 20005

Voice: 202-289-6868 (main)
202-289-2372 (Cochran)
FAX: 202-289-1060
Internet: TCochran@nrdc.org

Introduction

A one kiloton pure fission nuclear weapon can be fabricated with as little as one to three kilograms (kg) of plutonium or three to eight kg of highly-enriched uranium (HEU). There are roughly 300,000 kg of weapon-grade plutonium (WGPu) and some 2 million kilograms of HEU in nuclear weapon programs globally. Of these amounts over one-half (about 170,000 kg of WGPu and about 1.2 million kg of HEU) is in Russia, and about one-third to one-half of the Russian material is in some 20,000 intact weapons. Most of the remaining Russian materials are presumed to be in the form of warhead components in storage. In addition, Russia has about 30,000 kg of separated reactor-grade plutonium (RGPu) in storage.

Both the United States and Russia are retaining as strategic reserves more plutonium and HEU for potential reuse as weapons, than is legitimately needed. Both have engaged in discussions and have programs in various stages of development to dispose of excess plutonium and HEU. These fissile material disposition programs will take decades to complete. In the interim there will be, as there is now, hundreds of tons of separated weapon-usable fissile material stored in tens of thousands of transportable canisters, each containing from a few to several tens of kg of weapon-usable fissile material.

This material must be secured against theft and unauthorized use. To have high confidence that the material is secure, one must establish criteria against which the adequacy of the protective systems can be judged. For example, one finds such criteria in U.S. Nuclear Regulatory Commission (USNRC) regulations for the protection of special nuclear materials.

Requirements for the Protection Against Theft or Diversion of Weapon-Usable Nuclear Materials

In its regulations (10 CFR §73.1) the USNRC uses the concept of a "design basis threat" to judge the adequacy of the physical protection measures designed to prevent the theft nuclear weapon-usable materials. Licensees that possess or transport formula quantities of special nuclear materials are required to protect against:

> (i) A determined, violent, external assault, attack by stealth, or deceptive actions by a small group with the following attributes:
>
> > (A) Well-trained (including military training and skills) and dedicated individuals;
> > (B) Inside assistance that may include a knowledgeable individual who attempts to participate in a passive role (e.g.) provide information), and active role (e.g. facilitate entrance and exit, disable alarms and communications, participate in violent attack), or both;

(C) Suitable weapons, up to and including hand-held automatic weapons, equipped with silencers and having effective long-range accuracy;
(D) Hand-carried equipment, including incapacitating agents and explosives for use as tools of entry or for otherwise destroying reactor, facility, transporter, or container integrity or features of the safeguards system
(E) Land vehicles used for transporting personnel and their hand-carried equipment; and
(F) the ability to operate as two or more teams.

(ii) An individual, including an employee (in any position), and

(iii) A conspiracy between individuals in any position who may have: (A) access to and detailed knowledge of the [facilities], or (B) items that could facilitate theft of special nuclear material (e.g. small tools, substitute material, false documents, etc.) or both.

A “formula quantity” means strategic special nuclear material in any combination in a quantity of 5000 grams or more computed by the formula, grams = (grams contained U-235) +2.5 (grams U-233 + grams plutonium). In other words, the design basis threats above apply to the protection of more than 2 kilograms (kg) of plutonium, 2 kg of U-233, 5 kg of U-235, or any equivalent combination of these.

The first threat, described in (i) above, is call the “external” threat, while (ii) and (iii) are referred to as “insider” threats. The size of the “small group” in (i) is not defined in USNRC regulations. It used to be taken as six people, and perhaps the USNRC still uses this level as the design basis for the external threat. The conspiracy in (iii) is assumed to involve only two people.

The U.S. Department’s of Energy (USDOE) and Defense (USDOD) also use the same “design basis threat” approach to judge the adequacy of security at contractor operated facilities and for the transport of nuclear weapons, weapon components, and weapon usable materials. The USDOD and USDOE requirements are essentially equivalent to or exceed those prescribed in USNRC regulations.

A weakness of any security system, particularly where it concerns a potential theft by knowledgeable insiders, is that the threat can analyze the capability of the physical protection system and bring to bear the necessary people and equipment needed to overcome it and minimize the chances of being apprehended.

Since the dissolution of the Soviet Union in 1991 there have been break-ins at facilities in the former Soviet Union, but no reported incidences of external assaults, of the type described in (i) above, for the purpose of stealing formula quantities of special nuclear materials.

Between 1992 and 1994 there were several cases where single insider--case (ii) above--successfully removes kilogram quantities, but not formula quantities, of weapon-usable highly-enriched uranium (HEU). In each of the reported cases the individual was apprehended and the material recovered. At least one of these cases was a sting operation. When I last wrote about these cases in 1995, I offered the following observations which are still valid today:

> **1) Kilogram quantities of weapon-usable fissile materials have been stolen from institutes in Russia since the breakup of the Soviet Union.**
>
> **2) Some fraction of these materials was not intercepted before leaving the Russian borders.**
>
> **3) All known cases involved diversions from civil, space, and naval reactor research and fuel manufacturing facilities. No known diversions have occurred that involved nuclear weapons or weapon components.**
>
> **4) We don't know what we don't know. Given the lack of adequate inventory controls, there may well have been successful diversions that have not been detected.**

One should be cautious in drawing conclusions regarding the absence of reports since 1994 of serious cases—involving kilogram quantities of weapon-usable material—because the security and intelligence bureaucracies may be operating under different reporting guidlines. In any event the limited number of cases during the 1992-1994 period suggest that the single insider represents the most probable threat to illicit use of nuclear material.

It is generally agreed that the most cost effective way to protect of weapon-usable materials is to increase security at the source—where it is stored. Nevertheless, the fact that insiders have successfully removed kilogram quantities of weapon-usable material from FSU facilities points up the need to improve security across the board, including providing additional border security.

While the single insider (case (ii)) represents the most likely threat, in my view the most serious threat category is case iii, involving a collusion of security personnel and/or senior management at facilities storing significant quantities of weapon-usable material. Such a collusion could divert arsenal quantities of weapon-usable materials, and could market it with less chance of being apprehended.

Moreover, we should be more concerned about diversion scenarios where the recipient is a rogue state, rather than an individual or terrorist organizations. As demonstrated by the program in Iraq, a state can provide the financial and technical support needed to develop sophisticated nuclear weapons. In the case of an individual or terrorist organization, the consequences are usually described in terms of the damage of a single crude nuclear bomb. On the other hand a rogue state could construct an arsenal of sophisticated weapons. It is generally agreed by all experts within the arms control community that the pacing item in terms of a state's ability to obtain nuclear weapons is the acquisition of the fissile material. Purchasing the fissile material illicitly would reduce by years the time needed to acquire nuclear weapons. There would be little, if any, time available to bring diplomatic pressure, as in the case of North Korea, or for military intervention, as in the case of Iraq, if a rogue state secretly acquired kilogram quantities of fissile material from Russia by illicit means.

There is compelling evidence for concern over the possibility that a collusion of security and management personnel may become involved in the trafficking of arsenal quantities of plutonium or HEU. First, there was a case in 1993 involving the interception in Vilnius, Lithuania of four tonnes of beryllium that were diverted from a nuclear research institute at Obninsk in Russia.

There was a small incidental quantity of HEU involved but the amount was not significant, and for this reason many analysts have overlooked the significance of this case. The significance of the Vilnius case is that it had all the elements associated with the case (iii) scenario--the most worrisome scenario that potentially could involve the successful diversion of very large quantities of fissile material from Russia to the Middle East. Involved in this single case were a) at least one senior regional Russian government official, b) a senior official of a nuclear institute where tonne quantities of weapon-usable fissile materials are stored under inadequate physical security, c) an organization believed to be linked to the KGB and organized crime (mob) groups in Russia and Lithuania.

One other aspect of the Vilnius case is noteworthy. This case involved the shipment of four tonnes (2 cubic meters) of beryllium metal in 33 shipping crates. Each shipping crate was about 0.13 cubic meters (about five cubic feet) in volume. It would be very easy to hide a few kilograms of plutonium or HEU in such a shipment. Much larger shipments of metals are routinely exported from Russia legally. The Vilnius case demonstrates how easy it would be to divert enough plutonium or HEU for an arsenal of several nuclear weapons by hiding the fissile material among several tons of metal shipped in the course of a normal commercial transaction. It also demonstrates the importance of good border security.

Also, as noted by David Hoffman of *The Washington Post* (May 12, 1997, pp. 1, 15), since the collapse of the Soviet Union, the Russian Federation has failed to establish the rule of law. The judiciary is a weak and ineffective branch of government. People now speak of a fifth power--in addition to the executive, legislative, judiciary, and the press--namely, that of organized criminals. Former Soviet bureaucrats, factory directors, aggressive businessmen and criminal organizations have all made a grab for immense riches through inside deals, bribery and brute force. Private businessmen are building their own private armies of security agents, bodyguards and commercial spies. Former elite KGB troops are now operating private security forces to protect Russian businesses. Veterans of the Afghan and Chechen wars have been recruited as bodyguards. There has been a rash of contract killings. Many small businesses must pay for some kind of "krysha," a Russian slang word referring to criminal protection racket. Given these circumstances it is reasonable to conclude that the probability that present or former security personnel will become engaged in nuclear materials trafficking is sufficiently high to be quite worrisome. This threat must be taken most seriously.

To strengthen the nuclear material protection, control and accounting (MPC&A) at some 80 to 100 nuclear facilities at some 40 sites in Russia, in April 1994 the USDOE and its laboratories and nuclear institutes and enterprises of the Russian Federation launched a new program of cooperation on MPC&A. The program is called the Laboratory-to-Laboratory Nuclear Material Protection, Control, and Accounting Program (or simply the "Lab-to-Lab MPC&A Program"). This is one of a series of U.S./Russian bilateral MPC&A cooperative efforts, all designed to reinforce and complement the national MPC&A programs, particularly Russia's. The program has provided, and continues to provide, financial, material support and training to Russian facilities, including improved computerized accounting systems, a capability to measure nuclear materials in containers, access control systems, portal detectors, and various other types of monitoring and security equipment, including cameras, motion detectors, cameras and seals.

The Lab-to-Lab MPC&A program has been a highly successful cooperative effort. Progress during the first two years is summarized in "United States/Former Soviet Union Program of Cooperation on Nuclear Material Protection, Control, and Accounting, Department of Energy Nuclear Material Security Task Force, December 1996. Kenneth N. Luongo, who until very recently was Director of the Office of Arms Control and Nonproliferation of the USDOE, was in charge of the USDOE effort. Since Mr. Luongo is attending this conference I assume he will be discussing the successes and current status of the Lab-to-Lab MPC&A Program.

Without denigrating the remarkable success of the Lab-to-Lab effort, it nevertheless has its limitations. Coverage is not yet universal. Security experts from the U.S. labs do not have access to sensitive military facilities that need to be covered, and must rely solely on their Russian partners for improvements at these facilities. Perhaps most importantly, while the improvements should be most effective in protecting against the single insider threat, they will offer only minimal improved protection against a collusion of security and/or management personnel.

To provide more effective security at Russian nuclear facilities against a conspiracy of insiders, I believe it is now timely for the United States and Russia to complement the Lab-to-Lab effort by creating a more comprehensive bilateral program, with complete reciprocity, for inventory control, including joint maintenance in real-time of a fissile materials database that provides the location and the isotopic, physical and chemical properties of all excess weapon-usable fissile materials. Eventually this could become an IAEA responsibility, but to facilitate access to sensitive facilities and more rapid implementation the program should be initiated on a bilateral basis through thje Lab-to-Lab effort.

Such a program is also desirable if we are to achieve deep reductions in the nuclear weapon arsenals. Since about 1990 NRDC has been advocating that the United States and Russia (then the Soviet Union) engage in a nuclear weapons and fissile material data exchange as part of a program to verify the dismantlement of nuclear warheads. The Russian Foreign Ministry proposed a multilateral data exchange in 1992. Prodded by the U.S. Congress, the Clinton Administration agreed to initiate an exchange of nuclear weapons and fissile materials inventory data with the Russians in December 1994. The Yeltsin Administration accepted the concept a year later. On 10 May 1995 Presidents Clinton and Yeltsin issued a "Joint Statement on the Transparency and Irreversibility of the Process of Reducing Nuclear Weapons. Among the key provisions of this joint statement, the U.S. and Russia agreed to establish:

- An exchange on a regular basis of detailed information on aggregate stockpiles of nuclear warheads, on stocks of fissile materials and on their safety and security;

- A cooperative arrangement for reciprocal monitoring at storage facilities of fissile materials removed from nuclear warheads and declared to be excess to national security requirements to help confirm the irreversibility of the process of reducing nuclear weapons, recognizing that progress in this area is linked to progress in implementing the joint U.S.-Russian program for the fissile material storage facility at Mayak: and

- Other cooperative measures, as necessary to enhance confidence in the reciprocal declarations on fissile material stockpiles.

With respect to transparency, the Joint Statement also states that:

The United States of America and the Russian Federation will also examine and seek to define further measures to increase the transparency and irreversibility of the process of reducing nuclear weapons, including intergovernmental arrangements to extends cooperation to further phases of the process of eliminating nuclear weapons declared excess to national security requirements as a result of nuclear arms reduction.

The United States of America and the Russian Federation will seek to conclude in the shortest possible time an agreement for cooperation between their governments enabling the exchange of information as necessary to implement the arrangements called for above, by providing for the protection of that information. No information will be exchanged until the respective arrangements enter into force.

Unfortunately, in late-1995, without explanation, Russia cut off bilateral talks directed toward concluding an Agreement for Cooperation, the legal instrument that would permit the data exchange and transparency measures to go forward. There has been no progress between the United States and Russia on implementation of the agreed upon data exchange, or any warhead dismantlement and fissile material storage transparency and verification measures, except for language in the Helsinki Joint Statement of March 21, 1997 that “the two sides will also consider the issues related to transparency in nuclear materials.”

Russia’s refusal to move forward with an Agreement for Cooperation has brought to a halt virtually all reciprocal transparency initiatives related to nuclear warhead dismantlement and warhead component storage. It also denies the two sides a real opportunity to significantly improve fissile material security in Russia against the most serious potential threat—a collusion insiders involving security and/or management personnel.