# Reducing the threat of RDDs

by Charles D. Ferguson

*It's not enough to plug gaps in security systems for radioactive sources. Needed are integrated "cradle-to-grave" controls to prevent high-risk sources from finding their way into the wrong hands.*

The terrorist attacks of 11 September, 2001 sounded an alarm that ad hoc approaches to security do not provide adequate protection. By exploiting imperfections in the transportation security system, al Qaeda operatives were able to hijack four commercial airplanes on September 11.

Al Qaeda has also expressed interest in unleashing radiological terrorism by building and using radiological dispersal devices (RDDs) – one type of which is popularly known as a "dirty bomb." RDDs are not nuclear weapons and generally would not cause massive destruction. But they could spread radioactive particulates over wide areas. Although few people, if any, would die shortly after exposure to the ionizing radiation from a typical RDD, many could panic and become terrorized because of fears of radioactivity.

Common radioactive materials, such as commercial radioactive sources used in medicine, industry, and scientific research, could fuel RDDs. While the IAEA has worked toward improving the security of radioactive sources long before the September 11 attacks, the IAEA moved quickly after this date to increase its efforts to prevent these materials from becoming tools of radiological terror. IAEA Director General Mohamed ElBaradei has spoken often about the need for a "cradle-to-grave" protection system for radioactive materials. While the IAEA and several Member States have striven to establish such a system, more thinking and work are still required to develop an integrated, layered, and cooperative defense system for radioactive source security. *(See box: Global Call for Stronger Controls.)*

## Setting Priorities

Faced with the increased perceived security threat stemming from radiological terrorism, radiation safety and nuclear regulatory officials should resist the temptation to demand a high level of protection for all radioactive sources. Most of these sources do not require this level of security. Only a small fraction of the millions of radioactive sources used worldwide pose inherently high security risks, implying that security measures directed at these sources are manageable and can make rapid improvements in the overall security system. Nonetheless, this group in absolute numbers encompasses hundreds of thousands of sources, pointing out that security officials have to cope with a difficult challenge.

Factors determining the security risk of a type of radioactive source include prevalence of use, radioactivity content, portability, and dispersibility. Generally, the more prevalent, radioactive, portable, and dispersible a source is, the higher security risk it presents. For example, cesium chloride containing relatively large amounts of radioactive cesium-137 and consisting of an easily dispersible powder would definitely be categorized as a high security risk compound. If this material were also housed inside a portable container, a thief or terrorist could readily seize and transport the radioactive source if adequate security measures are absent.

Although dozens of different radioisotopes are employed in radioactive sources throughout the world, only about eight radioisotopes have characteristics that raise the sources containing them to the highest security risk level. (Each chemical element, such as cesium, comes in different forms called isotopes that have the same chemical properties, but different nuclear characteristics. Unstable isotopes, termed radioisotopes, try to transform into stable isotopic states by emitting radiation.)

The radioisotopes of highest security concern include the reactor-produced americium-241, californium-252, cesium-137, cobalt-60, iridium-192, plutonium-238, and strontium-90, as well as the naturally-occurring radium-226. The half-life (the time required for half the radioactive material to decay) of most of these radioisotopes is years to decades in length. (After seven half-lives, the radioactive substance has decayed to less than one percent of its initial amount.) Therefore, most of the high-risk radioactive sources will emit the majority of their radioactivity during a time period covering substantial parts of, or all of, a typical human lifespan. This fact explains part of the reason why radiological dispersal devices using these materials raise the risk level to human health.

***Security improvement should be prioritized on those radioactive sources that pose the greatest security risks.***

Other risk factors to human health stem from the ionizing radiation emitted by these eight radioisotopes. Four of the isotopes (americium-241, californium-252, radium-226, and plutonium-238) primarily release alpha particle radiation and would mainly pose internal health hazards via ingestion or inhalation because alpha particles are stopped by the dead layer of skin on a human body. Three of the other radioisotopes (cesium-137, cobalt-60, and iridium-192) result in the emission of high energy gamma radiation and would pose both external and internal health hazards because this radiation can easily pass though the body's dead layer of skin. Because strontium-90, the remaining radioisotope on this high-security list, emits high energy beta particles, it could pose an external health hazard in the absence of shielding. But it is primarily an internal hazard because, if ingested, it concentrates in bone.

Except for californium-252, these radioisotopes are used frequently in many applications, including teletherapy and brachytherapy cancer treatment, blood and food irradiation, industrial radiography, well logging, as well as level and thickness gauging. High security risk radioactive sources generally contain more than a few curies (or more than a few hundreds of Giga-Becquerel) worth of these radioisotopes.

The IAEA, in its *Categorization of Radiation Sources*, first published in July 2000, and in other Agency documents and statements, has recognized that security improvements should be prioritized on those radioactive sources that pose the greatest security risks, such as those described above. Regulatory agencies in many Member States have also placed emphasis on focusing security enhancements on this class of sources. What does an effective security system for these sources entail?

## Establishing a Layered and Integrated Security System

Perfect security systems do not exist. After imperfections in a security system are exploited, authorities tend to overreact by plugging the exposed gap in the system while often neglecting other gaps. Although repairing such gaps is necessary, this work should not take away from development of a layered and integrated security system.

A layered security system means that multiple barriers are in place to lessen the likelihood of a radiological terror act. The more security barriers the more likely a terrorist would be deterred from seizing radioactive materials because the chances that a terrorist would be caught increase. With one layer of protection, determined terrorists would probably be able to find a way around this barrier. Added layers would frustrate terrorists' attempts to break through the security system.

An integrated security system means that adequate layers of security protect every stage of a high-risk radioactive source's lifecycle from cradle to grave. This lifecycle begins with production of radioisotopes in nuclear reactors. (Although many radioisotopes are also produced in particle accelerators, these isotopes tend to be short-lived and, therefore, do not pose high security risks. The other exception, as discussed above, is radium-226, which occurs naturally.)

Most of the production reactors are government-owned research reactors, though there are a couple of privately-owned production reactors. Standard government-required security measures generally provide strong layers of protection at the reactor sites. These layers typically include fences, truck barriers, access control points, and guards.

After radioisotopes are produced, they are processed into radioactive sources. Much of this processing occurs at the reactor sites. Thus, the layers of protection at these sites apply at this lifecycle stage.

Transportation from the reactor and processing sites removes the radioactive material from the physical security system surrounding these facilities. Nonetheless, high security measures are in place for large shipments of highly radioactive materials. Layered protection includes multiple means of continuously monitoring the shipments and rapid notification to law enforcement officials if security problems arise.

In the United States, for example, the Nuclear Regulatory Commission (NRC) coordinates closely with the Department of Transportation in determining additional security requirements. To determine the transportation industry's compliance with security standards in the United States, the NRC conducts inspections and increased the frequency of these inspections about a month after 11 September, 2001. Some security experts have recommended conducting criminal background checks of transportation personnel.

Radioisotope producers and processors transport radioactive sources to companies that manufacture equipment incorporating the sources. Security practices at the equipment manufacturing facilities tend to be based on standard industrial measures to protect high-value materials. While these practices generally provide adequate security, they may not be as strong as those used to guard large shipments. Frequent and random regulatory agency inspections should occur to ensure sufficient security is in place at the equipment manufacturing sites.

The next stage in a source's lifecycle involves employment by a user in an application, such as food irradiation, medical instrument sterilization, cancer treatment at a hospital, industrial radiography, well logging at a geological site, or scientific research at a university. Because food irradiation and medical instrument sterilization use massive amounts of highly radioactive materials, the highest security measures are usually in place at facilities carrying out these activities. Security at facilities carrying out the other applications is typically based on standard practices to protect high-value items. These practices could entail a number of protective layers, including restricted access, guards, requirements to lock up sources when not in use, and procedures for ensuring trusted personnel are monitoring sources when in use.

Security vulnerabilities depend significantly on the type of application and facility. For example, some facilities such as many hospitals and universities, are well-trafficked and purposely open to the public. Other facilities, such as many industrial sites where radiography and well logging are employed, are often in remote and relatively inaccessible locations. This situation may decrease the likelihood that malicious individuals could find and seize the radioactive sources. However, the transnational character of some industries, especially the oil industry, may increase the likelihood that sources will become lost or stolen.

Once radioactive sources are no longer needed to perform their intended function, they are known as disused sources. Depending on the radioactive material's properties, disused sources can remain potent and thus pose a security concern for an appreciable period of time.

Ideally, users would send sources soon after they are no longer useful to safe and secure disposal facilities operated by major source manufacturers or governments. High disposal costs and lack of adequate disposal facilities can discourage users from promptly and properly disposing of disused sources. The longer a disused source remains at a user's facility the more vulnerable it is to theft and diversion.

Major manufacturers generally provide some means of disposal often in exchange for a new source. However, this pathway toward proper disposal can be cut off if companies go out of business or stop providing the disposal service.

Government-operated disposal facilities can provide another means to safely and securely dispose of disused sources. However, many States do not have such depositories or have disposal storage sites that will only accept certain types of disused sources, such as those with relatively low levels of radioactivity.

A proposed concept for creating adequate global depositories is to set up regional facilities that States within a region can share. However, obtaining approval of depository construction might prove difficult unless States develop a fair means of burden sharing. For instance, States without the depositories might consider paying higher fees than States with the depositories in exchange for not having depositories on their territories. In general, an effective fee system is needed to fund disposal facilities. A proposal is to have users pay part or all of the disposal cost during the purchase of the radioactive source.

Radioactive sources that do not follow the ideal lifecycle that ends in disposal at secure depositories risk

becoming orphaned. Orphan sources are outside of regulatory controls because they have been lost, stolen, or abandoned. They represent failures of the safety and security system. About 500,000 of the two million sources in the United States, for example, may no longer be needed and thus are susceptible to becoming orphaned.

Although orphan sources exist in many advanced industrialized States, such as the U.S., this problem is most severe in the States of the former Soviet Union. Estimates are that thousands of high-risk orphan sources are strewn about this region. Illicit trafficking and terrorist activity in this region further increase the security risks.

A layered defense system focused on this problem would build upon the efforts begun by the IAEA and other Member States. In particular, the trilateral initiative started last year among the IAEA, the Russian Ministry of Atomic Energy, and the U.S. Department of Energy to track down orphan sources can hopefully prove to be a model of cooperation in this field. To make this happen, the parties involved need high level political support, sufficient funding, adequate detection equipment, and thorough searching of radioactive source records from the former Soviet Union.

Additional elements of a layered and integrated defense system include ensuring the legitimacy of users and employing radiation detectors at border crossings and high-profile locations. Checking on the legitimacy of users should involve detailed governmental reviews of imports and exports as well as domestic activity.

## Striving for Cooperative Security

Some radioactive source industry officials have expressed concern that security costs will keep ratcheting up and will never go back down. If this process were the only economic dynamic in play, this industry would clearly be at a disadvantage compared to manufacturers of non-radioactive alternatives to radioactive sources. In this hypothetical scenario, further security costs could tend to drive some radioactive source companies out of business. Another possibility is that these companies, in order to survive, might cut back on security to save costs. Either scenario leads to undesirable consequences.

Improved radioactive source security should not necessarily result in loss of business. Companies and regulators should continue to work closely with each other to build a security system that does not dismantle business. A truly layered and integrated defense system can instill confidence in consumers. Such confidence might then lead to greater acceptance of radioactive sources, promoting growth of this business.

Users should also factor in the principle of justification when deciding whether to buy a radioactive source or a non-radioactive alternative. This key principle of radiation protection weighs the benefits versus the risks of using a radioactive source. Sometimes a non-radioactive alternative can provide comparable benefits without high safety and security risks. Other times a radioactive source may suit the particular application better than a non-radioactive alternative.

***More thinking and work are still required to develop an integrated, layered and cooperative defense system for radioactive source security.***

Industry and governments should consider forming private-public partnerships that could conduct research and development aimed at enhancing radioactive source security. Part of this research should involve systems analysis that would search for security system vulnerabilities and would identify ways to erect layered defenses.

Industry, governments, and the IAEA face many challenges in striving to develop an effective integrated, layered, and cooperative security system for radioactive sources. Though these challenges appear daunting, prioritizing security improvements on the high-risk radioactive sources will make great strides toward reducing the risk of a radiological dispersal device attack.

*Charles Ferguson is Scientist-in-Residence, based in the Washington, DC, office of the Center for Nonproliferation Studies (CNS), Monterey Institute of International Studies. He co-wrote, along with Tahseen Kazi and Judith Perera, "Commercial Radioactive Sources: Surveying the Security Risks," Occasional Paper No. 11, CNS, January 2003. Parts of this Bulletin article are based on this paper. E-mail: charles.ferguson@miis.edu.*

# GLOBAL CALL FOR STRONGER CONTROLS

US Energy Secretary Spencer Abraham, IAEA Director General Mohamed ElBaradei and Austrian Minister for Foreign Affairs B. Ferrero-Waldner at the March event. *(Credit:Calma/IAEA)*

Over 700 delegates from more than 120 countries gathering in Vienna in March 2003 called for stronger national and international security over radioactive sources, especially those that could be used to produce a terrorist "dirty bomb."

"High-risk radioactive sources that are not under secure and regulated control, including so-called 'orphan' sources, raise serious security and safety concerns," the International Conference on Security of Radioactive Sources concluded. "Effective national infrastructures for the safe and secure management of vulnerable and dangerous radioactive sources are essential for ensuring the long-term security and control of such sources."

In some countries, regulatory control of radioactive sources — used extensively in medicine and industry — remains weak. Global concerns about the security and safety of radioactive sources escalated following the September 2001 terrorist attacks in the United States. There are fears that some radioactive sources could be used by terrorists as radiological dispersal devices, or so-called "dirty bombs."

"Source security has taken on a new urgency since 9/11," Dr. Mohamed ElBaradei, Director General of the International Atomic Energy Agency said during the conference opening. "There are millions of radiological sources used throughout the world. Most are very weak. What we are focusing on is preventing the theft or loss of control of the powerful radiological sources," Dr. ElBaradei said.

To effectively deal with the potential terrorist threat posed by so-called dirty bombs, the conference called for new international initiatives aimed at facilitating the location, recovery and securing of high-risk radioactive sources throughout the world, under the aegis of the IAEA. The Conference also called for a concerted worldwide effort under IAEA leadership to implement the principles in the Code of Conduct on the Safety and Security of Radioactive Sources, which is now being revised to account for security concerns, in order to promote adequate radiation safety and security control infrastructures. States should also adhere to the security-related principles contained in the international Basic Safety Standards that the IAEA has issued.

The Conference has offered numerous specific findings for addressing security concerns, identifying high-risk sources, and strengthening government actions to minimize radiological risks. Among the key recommendations:

- ✔ Implementation by all States of national action plans for locating, searching for, recovering and securing high-risk radioactive sources;
- ✔ Strengthening measures to detect, interdict and respond to illicit trafficking in high-risk radioactive sources;
- ✔ Public awareness campaigns to foster - among legislators, source users and the public - a better understanding of real threats and the appropriate responses in the event of a radiological emergency;
- ✔ Concerted efforts by all States and the IAEA to enhance the current national and international arrangements to respond proactively to the possible malevolent use of high-risk radioactive sources.

"It is our critically important job to deny terrorists the radioactive sources they need to construct such RDD weapons," United States Energy Secretary Spencer Abraham told the Conference. "Our governments must act to identify all the high-risk radioactive sources that are being used and have been abandoned. We must educate our officials and the general populace, raising awareness of the existence of these dangerous radioactive sources and the consequences of their misuse."

The International Conference on Security of Radioactive Sources was held from 10 to 13 March 2003 at the Hofburg Palace in Vienna, Austria. U.S. Secretary of Energy Spencer Abraham presided over the Conference, which was co-sponsored by the Government of the Russian Federation and the Government of the United States of America and hosted by the Government of Austria. It was organized by the IAEA in co-operation with the European Commission, the World Customs Organization, the International Criminal Police Organization (ICPO-Interpol) and the European Police Office (Europol).

For more information, including the Conference Findings, visit the IAEA's web site at http://www.iaea.org/worldatom/Press/Focus/RadSources/index.shtml