April 2015

CNS Global Incidents and Trafficking Database

Tracking publicly reported incidents involving nuclear and other radioactive materials

2014 Annual Report

Produced Independently for the Nuclear Threat Initiative by the James Martin Center for Nonproliferation Studies

Contents

Acknowledgments

The 2014 Report was authored by Benjamin Pack and Bryan Lee with research assistance from Amaury Crucy, Anthony Sisneroz, Margarita Colon, Paul A. Kynerd, and Ruby Russell. The authors are also grateful to Dr. George Moore for his valuable feedback on an earlier version of this text.

Executive Summary

Nuclear and radiological terrorism are real and global threats. The detonation of a crude nuclear bomb would cause catastrophic harm to human life and infrastructure. The political and economic consequences would extend well beyond the blast site, impacting nearly every country worldwide. Terrorists would find it extremely difficult, but not impossible, to carry out a nuclear attack. An attack involving a radiological weapon would be far easier for terrorists to execute. Although unlikely to result in many casualties, it could still cause substantial property damage through contamination and incite mass panic by provoking people's fear of radiation.

Without the necessary materials to build a nuclear or radiological device, terrorist cannot carry out a nuclear or radiological attack. Maintaining control over these materials globally is vital to preventing nuclear and radiological terrorism. Yet, as the CNS Global Incidents and Trafficking Database shows, with so much radioactive material in use worldwide, control is routinely compromised.

Over the past two years, the CNS database has identified ***325 publicly reported incidents across 38 different countries*** (155 in 2013 and 170 in 2014) in which nuclear or other radioactive material was lost, stolen, or otherwise outside of regulatory control. ***Fortunately, few incidents involved material that was directly weapons-usable.*** Weapons-usable nuclear material was identified in just one incident, which involved less than a gram of highly enriched uranium, and only 5 percent of cases involved high-risk radioactive sources.

The dearth of truly high-risk incidents, however, does not necessarily indicate that weapons-usable materials are adequately secure. Indeed, most incidents were caused by careless, not criminal, individuals; and even among cases linked to criminal activity, many often involved the unintentional or opportunistic theft of radioactive material. If petty criminals can exploit weak security controls or careless human behavior, then certainly an organized and determined terrorist group can as well.

Building upon last year's analysis, this report examines five key findings from the data with corresponding policy implications for how governments, regulatory authorities, and industry can improve their capacity to understand, mitigate, and prevent future and potentially more serious incidents.

(1) Dataset: Tip of the Iceberg?

It is likely that many more incidents occur than are detected and/or reported due to wide variations in national regulatory capacity, reporting norms, and transparency. In some countries with large nuclear or other radioactive materials holdings, few incidents were reported, and the majority of those reports came from the media rather than the national regulatory authority. Conversely, more than 70 percent of reported incidents came from the United States, Canada, and France, and almost all incidents were publicly reported by their respective regulatory authorities.

Improving Reporting through Capacity Building

Improving public reporting worldwide would undoubtedly raise awareness of the threat and provide more information to develop effective policy solutions. While some governments may fail to report incidents of which they are aware, others simply lack the capacity to regulate radioactive materials effectively. Establishing and cultivating capacity building programs in countries where poor reporting is the result of limited regulatory capabilities offers the most promising avenue for improved reporting globally.

(2) No Nexus between Trafficking & Terrorism…Yet

Although the data does not indicate a convergence between illicit trafficking, organized crime, and terrorism, such a nexus may one day emerge. Just because a terrorist nuclear or radiological attack has not yet occurred does not mean one is not possible. Traffickers operating in some parts of the world remain attracted to the perceived value of illicitly acquiring and selling radioactive material. A wide variety of actors, from petty smugglers to organized criminal groups, are involved in the illicit transfer and sale of these materials, particularly in Eastern Europe and Eurasia.

Targeting Law Enforcement Training and Cooperation

Given limited resources, governments should work to improve intelligence and law enforcement cooperation in regions where radioactive material smuggling is prevalent, emphasizing the tools that have proven most effective in detecting and disrupting these activities, such as sting operations and incentives to encourage informants to come forward. Countries should also work to ensure that states around the world have strong legal frameworks in place to criminalize and effectively prosecute individuals involved in the theft or smuggling of radioactive materials. The risk of capture and prosecution is unlikely to dissuade terrorists from engaging in these activities; but since most traffickers today appear to be profit-motivated, strong penalties could serve as a deterrent.

(3) Transport & Physical Security Vulnerabilities

In lieu of finding illicit sellers, terrorists might also look to steal radioactive material directly from one of the thousands of locations where it is stored, used, and disposed of. ***In particular, the dataset suggests materials are particularly vulnerable during transport. Over twice as many thefts occurred during transit than at fixed locations.***

Strengthening Regulation & Recovery Methods

Multiple incidents occurred despite the fact required security controls appeared to have been in place, suggesting the need for additional regulation, particularly for materials in transit. Yet strong security involves not only measures to prevent loss of control, but also mechanisms to re-establish control in the event preventive measures fail. Efforts to recover lost or stolen materials, if and when they were successful, relied heavily on manual searches, anonymous tips, and a fair bit of luck. Some countries have explored the feasibility of tagging and tracking radioactive sources via electronic means. While there remain technical and cost issues associated with these technologies, the CNS incident data underscores their potential value and gives reason to support continued investment in these projects.

(4) Human Error: A Dangerous Culprit

The majority of incidents captured over the past two years resulted from avoidable human negligence, such as forgetting to lock up radioactive sources, communication breakdowns during transfer and shipment, and lax inventory controls.

Addressing Negligence through Security Culture

The widespread and often daily use of commercial radioactive sources at universities, hospitals, and construction sites limits the applicability of traditional "gates, guns, and guards" approaches to security. This reality, combined with the apparent role of human error in many reported incidents, highlights the importance of developing a strong security culture at all sites where nuclear and radiological materials are present. A combination of improved training and guidance, more frequent best practice exchanges, and enhanced end-user accountability can help minimize the number of future incidents attributable to human negligence.

(5) Room for Radioactive Source Minimization

Many reported incidents involved radioactive sources used in applications for which non-radioactive alternatives exist. Non-radioactive alternatives can lower and even eliminate the particular manufacturing, transportation, and disposal costs that arise precisely because of the safety and security concerns associated with managing radioactive sources throughout their life-cycle.

Studying & Incentivizing Non-radioactive Alternatives

Although safer alternatives can reduce security risks and lessen regulatory burdens, some may not be practical or economically viable today. As greater attention is given to radioactive source minimization and replacement, governments should perform comprehensive cost-benefit analyses of select cases to determine if conversion is warranted, and prepare to offer assistance to encourage suppliers to move to alternative technologies and dispose of obsolete sources.

Conclusion

This 2014 report on the CNS Global Incidents and Trafficking Database reinforces last year's findings. Varied reporting transparency continues to obscure the scale of the threat posed by illicit trafficking, while lapses in physical security and human error enable trafficking incidents to take place. Making progress on these three key fronts should be a top priority for governments seeking to reduce the risk of nuclear and radiological terrorism.

I. Introduction

Nuclear and radiological terrorism are real and global threats. The detonation of a crude nuclear bomb in a major city would have catastrophic consequences, reducing infrastructure to radioactive rubble and leaving perhaps thousands of people dead. Terrorist use of a radiological weapon would be far less devastating—with a death toll likely limited to the single or double digits—but could still result in significant social and financial costs.[1] Not only might such an event cause substantial property damage through contamination, requiring costly and time-consuming cleanup, but it would likely incite mass panic by provoking people's fear of radiation. Thus, while radiological weapons may not be weapons of destruction, they are more accurately described as weapons of mass disruption.

Terrorists cannot carry out an act of nuclear or radiological attack unless they can access the necessary ingredients to build a bomb. Thus, securing nuclear or other radioactive material globally and reestablishing control over stolen, lost, or abandoned materials is vital to the prevention of nuclear and radiological terrorism. The CNS Global Incidents and Trafficking Database prepared by the James Martin Center for Nonproliferation Studies (CNS) and funded by the Nuclear Threat Initiative (NTI) offers researchers and policymakers a unique resource to assess the nature and scope of nuclear security risks. Several international organizations and research institutions maintain similar products, but no other database of this type is both globally comprehensive and freely available to the public.[2] The International Atomic Energy Agency's (IAEA) Incident and Trafficking Database (ITDB) is the most well-known. However, it only contains incidents that are reported or confirmed by participating states, and does not share incident details publicly. Other databases, such as the Database on Nuclear Smuggling, Theft, and Orphan Radiation Sources (DSTO) maintained at the University of Salzburg, track government-reported cases as well as incidents reported elsewhere in open sources, but are only accessible with permission from their owners.

Relying on a mix of governmental and non-governmental sources, the CNS database tracks open-source reporting on incidents involving the loss of regulatory control over any nuclear or other radioactive material requiring such control. Its scope covers intentional criminal acts, such as theft and unauthorized possession, as well as unintentional acts, such as losses, misrouted deliveries, or accidental discovery. Capturing both types of incidents is important because each incident has security implications. Whether loss of control is the result of theft or negligence, the associated materials are now hypothetically available for unauthorized purposes, including criminal or terrorist acts. Moreover, the circumstances surrounding any loss of control may illuminate vulnerabilities and enable policymakers, regulators, law enforcement officials, and other relevant authorities to take corrective actions to prevent more serious diversion of materials in the future.

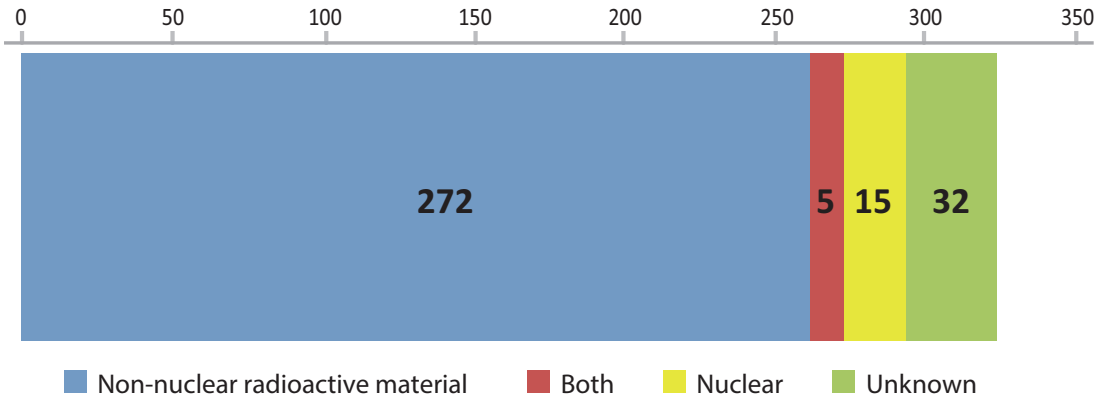
The initial 2013 Annual Report highlighted six key findings and corresponding policy implications. This 2014 report builds on those findings and introduces several new issues. Although the database remains a work in progress and it is too early to identify long-term trends, the findings presented here have potential policy implications for how governments, regulatory authorities, and commercial end-users can improve their capacity to understand, mitigate, and prevent future incidents. These initial findings will be monitored as more data are accumulated, and corresponding policy implications will be reassessed and refined annually.

[1] U.S. Nuclear Regulatory Commission, "Fact Sheet on Dirty Bombs," December 12, 2014, https://forms.nrc.gov/reading-rm/doc-collections/fact-sheets/fs-dirty-bombs.html.
[2] For an overview of other databases, see 2013 Annual Report, p. 1-2.

II. Weapons, Materials, and Data Overview

Terrorists cannot build a nuclear or radiological device unless they can acquire the necessary materials. For a terrorist-constructed nuclear weapon, commonly termed an improvised nuclear device (IND), this means acquiring kilogram quantities of fissile materials, namely highly enriched uranium (HEU) or separated plutonium. Radiological weapons could by definition employ any type of radioactive material, whether nuclear or non-nuclear, but of the several thousand that exist, only about a dozen exhibit characteristics—such as half-life, radioactivity, portability, dispersibility, and availability—that make them a security threat.

Figure 1. Reported Incidents by Material Type



Nuclear Material

Incidents involving nuclear material—defined as various forms, or isotopes, of plutonium, thorium, and uranium—account for less than 10 percent of the dataset. The vast majority of these incidents involved low-grade materials, such as natural uranium ore, yellowcake, and depleted uranium. None of the incidents captured over the past two years involved separated plutonium. In 2014, the database recorded its first credible HEU incident involving an instrument which went missing at a U.S. nuclear power plant; however, the device contained only miniscule quantities of material, about four one-thousandths of a gram (Incident #2014245).

The low number of reported incidents involving weapons-usable nuclear material is consistent with the findings of other data holdings. Over the last two decades, the IAEA has documented only 16 cases of unauthorized possession of HEU or plutonium, with an additional 3 credible incidents documented in the open-source but not confirmed to the IAEA by relevant member states.[3] The low number of reported incidents involving weapons-usable nuclear material is at least in part a reflection of the more robust security mechanisms for nuclear versus other radioactive materials. All of these incidents reportedly involved material that was stolen long ago—prior to or around the time the United States and other countries began to give increased attention to addressing the threat of nuclear terrorism. [4]

[3] As of December 2013, 16 cases of unauthorized possession of HEU or plutonium had been reported to the IAEA. The Database on Nuclear Smuggling, Theft, and Orphan Radiation Sources (DTSO), which tracks both official and unofficial reports, had identified 19 credible incidents through 2012. See International Atomic Energy Agency, "IAEA Incident and Trafficking Database (ITDB)," Fact Sheet, 2014, www.iaea.org; Lyudmila Zaitseva and Friedrich Steinhäusler, "Nuclear Trafficking Issues in the Black Sea Region," EU Non-Proliferation Consortium Papers, No. 39, April 2014, p. 4, www.sipri.org.

[4] "Illicit Trafficking in Weapons-Useable Nuclear Material: Still More Questions Than Answers," Center for Nonproliferation Studies, December 11, 2011, www.nti.org.

Catalyzed by the collapse of the Soviet Union and then by 9/11, global concern over nuclear security has produced a host of international instruments and cooperative initiatives which have led many countries to upgrade security measures at sites housing weapons-usable nuclear material, consolidate material holdings to fewer locations, and even eliminate their stocks entirely.[5] Despite substantial improvements, these efforts do not yet add up to a system that ensures all nuclear weapons and weapons-usable nuclear material are effectively protected against terrorist and criminal threats.[6] Moreover, it remains difficult to assess the degree to which more serious nuclear material incidents go unreported or undetected. Not all nuclear traffickers are caught; even more fundamentally, poor nuclear material accountancy in some countries makes it impossible to even know whether nuclear material is missing, let alone in what forms and/or quantities.

Other Radioactive Material

The vast majority, about 85 percent, of recorded incidents in the database involved non-nuclear radioactive material. From the perspective of radiological terrorism, about a dozen types of radioactive material are commonly identified as posing a security concern.[7] One type of radiological weapon, known as a radiological dispersion device (RDD), is designed to spread radioactive material into the environment to expose people to radiation or contaminate an area with radioactivity. Since RDDs rely on external exposure to cause harm, they require materials that emit deeply penetrating gamma or moderately penetrating beta radiation to be effective, such as cesium-137, cobalt-60, iridium-192, and strontium-90. Of these, the most frequently documented material is cesium-137, which appeared in about 30 percent of cases recorded in the dataset, followed by iridium-192 (6.5 percent), strontium-90 (2.7 percent), and cobalt-60 (2.4 percent).

Another often overlooked method of radiological terrorism involves what one group of experts dubbed "inhalation, ingestion, and immersion (I^3) attacks."[8] These attacks rely not on external exposure, but rather on a radioactive substance actually entering the human body to deliver a direct internal dose of radiation. While some low-penetrating radioactive materials, or alpha-emitters such as polonium-210, do not pose a threat when *outside* the human body, once internalized, they are lethal even in miniscule, sometimes microgram-quantities.

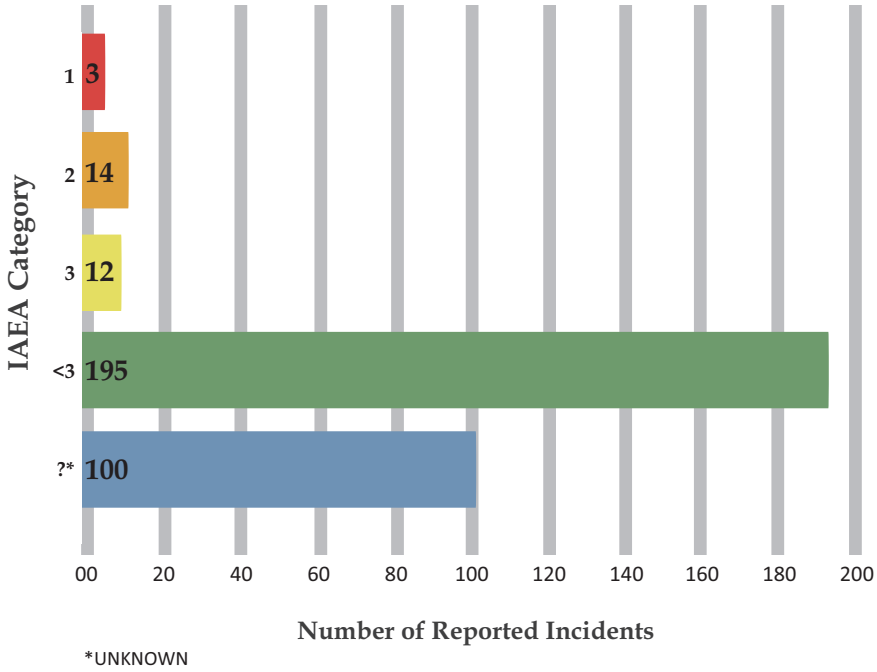
Although only gram-sized quantities of radioactive material would be required to make a radiological weapon, most of the cases captured in the database do not involve material quantities large enough to pose a security threat on their own. Radioactive materials are most commonly found in commercial "radioactive sources," which are used in every country for a wide variety of industrial, medical, and research applications. In most sources, radioactive material is sealed inside a protective casing to prevent accidental exposure (Figure 2).

The International Atomic Energy Agency (IAEA) categorizes radioactive sources according to their safety and security risks on a scale from 1-5, with Category 1 sources presenting the greatest health risk and Category 5 the lowest.[9] Most countries use this categorization scheme to develop national-level regulations. Few

[5] For more information on the history and state of the global nuclear security architecture, see the 2013 Annual Report p. 10-11; Matthew Bunn, Martin B. Malin, Nickolas Roth, and William H. Tobey, Advancing Nuclear Security: Evaluating Progress and Setting New Goals, (Cambridge, MA: Report for Project on Managing the Atom, Belfer Center for Science and International Affairs, Harvard Kennedy School), March 2014.
[6] For an in-depth assessment of the nuclear materials security conditions around the world, see Nuclear Threat Initiative and Economist Intelligence Unit, NTI Nuclear Materials Security Index: Building a Framework for Assurance, 2nd Edition, January 2014, www.ntiindex.org.
[7] Charles D. Ferguson, Tahseen Kazi, Judith Perera, "Commercial Radioactive Sources: Surveying the Security Risks," Occasional Paper No. 11, Center for Nonproliferation Studies, January 2003, www.nonproliferation.org.
[8] James M. Acton, M. Brooke Rogers, and Peter D. Zimmerman, "Beyond the Dirty Bomb: Re-thinking Radiological Terror," *Survival: Global Politics and Strategy* 49, No. 3, (Autumn 2007), p. 151-168.
[9] International Atomic Energy Agency, "Categorization of Radioactive Sources," *IAEA Safety Standards Series RS-G-1.9*,

incidents captured in the CNS database involved the most dangerous radioactive sources. Only three Category 1 "extremely dangerous" cases were reported in 2013 and none were recorded in the 2014 dataset. Four and ten cases of "very dangerous" Category 2 sources were reported in 2013 and 2014, respectively.

Figure 2. Incidents by IAEA Category, 2013-2014



Sealed radioactive source, Image Source: GAO

Most experts agree that Category 1 and 2 sources are genuinely high risk, but there remains significant debate over whether the IAEA categorization scheme (and consequently national regulations) adequately captures the threat posed by lower category sources. Indeed, as the IAEA notes, the scheme is based only on the immediate risks to human health, and does not take into account "socioeconomic consequences resulting from radiological accidents or malicious acts [because] the methodology to quantify and compare these effects, especially on an international basis, is not yet fully developed."[10] Although few, if any, causalities would result from exposure to radiation in the event of an RDD attack involving a Category 3 source, it could still cause significant property damage depending on the dispersal method and the location of the attack.[11]

In addition, the IAEA categorization scheme does not "factor in the ease of access to and transport of various sources."[12] Devices containing Category 1 sources, such as a blood irradiator shown in Figure 3(a), tend to be much larger than those at lower levels, and once installed, generally remain stationary, making loss or theft far less likely while they are in use.[13] Indeed, the vast majority of radioactive sources that fall outside of regulatory

Vienna, 2005, www.iaea.org.
[10] International Atomic Energy Agency, "Categorization of Radioactive Sources," *IAEA Safety Standards Series RS-G-1.9*, Vienna, 2005, p. 37, www.iaea.org.
[11] Charles Ferguson, "Ensuring the Security of Radioactive Sources: National and Global Responsibilities," USKI Working Paper Series, US-Korea Institute at SAIS, March 2012, p. 8, www.fas.org
[12] Charles Ferguson, "Ensuring the Security of Radioactive Sources: National and Global Responsibilities," USKI Working Paper Series, US-Korea Institute at SAIS, March 2012, p. 8, www.fas.org.
[13] A terrorist group could remove a Category 1 radioactive source from a large device like a blood irradiator, but to do so would need design information, tools, and proper shielding to protect themselves from lethal doses of radiation. While such challenges make theft unlikely, they arguably make the threat of sabotage while the device is in use much greater.

control are relatively small, mobile devices. For example, lost iridium-192 radiography cameras like the one shown in Figure 3(b) accounted for most of the incidents involving Category 2 sources. These portable industrial devices are used to examine structures such as pipelines for safety and quality control purposes. Most of the recorded Category 3 incidents involved iridium-192 brachytherapy devices used in cancer treatments and designed to be small enough to be inserted in or near a cancerous tumor. Moisture density gauges, as shown in Figure 3(c) and typically containing less than Category 3 sources of cesium-137 and americium-241, were involved in more incidents than any other type of device. These gauges are used in a wide variety of industrial applications, and in many cases, at remote or temporary locations requiring frequent transport to and from a job site. Terrorists might find devices like these more attractive given the relative ease with which they can be handled and concealed.

Figure 3. Images of Radioactive Sources

Figure 3:
(a) Blood irradiator containing a Category 1 source of cesium-137, Source: GAO
(b) Industrial radiography camera with a Category 2 source of iridium-192, Source: GAO
(c) Moisture density gauge, which typically contains less than Category 3 sources of cesium-137 and americium-241, Source: NRC.gov

Lastly, several experts argue the IAEA categorization scheme underestimates the risks associated with alpha sources, which make for poor RDDs but are ideal for so-called I[3]-style attacks. Since the scheme is based only on external radiation exposure (or so called "pocket doses"), low-penetrating alpha sources are typically relegated to Category 4 or 5, and are thus "often among the least well protected."[14] For example, polonium-210 is often found in a device called a static eliminator, which is typically a Category 4 source. The CNS database identified 4 incidents involving lost polonium-210 static eliminators in 2013 and 3 incidents in 2014. Three of these incidents involved devices containing twenty times the lethal dose of polonium-210.[15] One incident from 2014 involved the loss of 11 static eliminators, which cumulatively contained twenty-five times the lethal dose (#2014261). Most of these devices were not recovered.

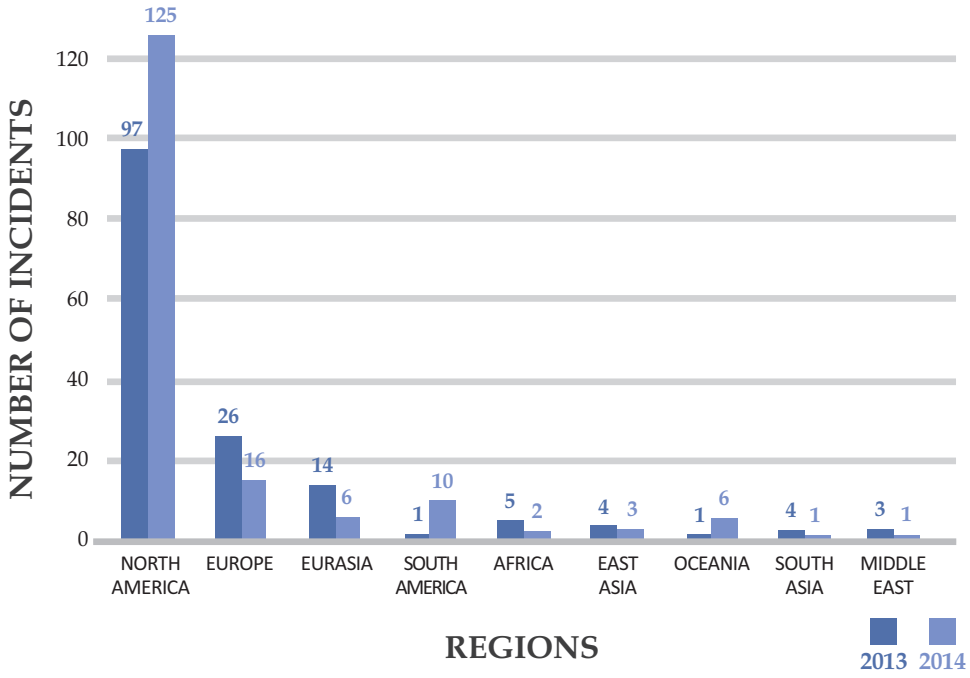
[14] James M. Acton, M. Brooke Rogers, and Peter D. Zimmerman, "Beyond the Dirty Bomb: Re-thinking Radiological Terror," *Survival: Global Politics and Strategy* 49, No. 3, (Autumn 2007), p. 155.
[15] See Incident #2013129, #2013028, and #2014270.

III. Key Findings and Policy Implications

Key Finding 1: Highly Variable Reporting Transparency

Over the past two years, the CNS database identified 325 incidents occurring in 38 different countries. 155 cases in 28 countries and 170 cases in 28 countries were reported in 2013 and 2014, respectively. The majority of incidents, about 58 percent, occurred in the United States, followed by Canada (9 percent), France (6 percent), Russia (3 percent), and Australia (2 percent). A state regulatory authority issued an annual or regular incident report to the public in just 5 countries: Australia, Belgium, Canada, France, and the United States.

Figure 4. Reported Incidents by Region



The data presents an incomplete picture, but the uneven geographical distribution of incidents suggests uneven levels of detection and/or reporting by national regulatory authorities. In some countries with large nuclear or other radioactive material holdings, few incidents were reported, and in most instances, were reported by the media rather than the national regulatory authority. For example, only 10 incidents were reported in Russia, 3 in Brazil, and 2 each in China, India, and Japan over the past two years. These low numbers are particularly striking in that they are comparable to the number of reported cases in small countries—such as Malta (1), Nepal (1), and Costa Rica (1)—that lack advanced nuclear sectors and make comparatively limited use of radioactive sources.

The large number of incidents reported in only a small number of countries should not be understood as implying that trafficking is a greater problem in those countries with more reported incidents, or that they face greater challenges in maintaining control over radioactive material. Strong material accountancy standards and a culture of transparency may have resulted in more incidents being reported to and by these countries' regulatory authorities. Likewise, the dearth of reported incidents in certain countries does not always imply that the country has an effective security system; many more incidents may occur than are detected and/or reported , whether due to capacity deficits, a weak culture of transparency, or some combination of the two.

Policy Implication 1: Improving Reporting through Capacity Building & Education

Improving public reporting of incidents and trafficking worldwide would increase overall understanding of the problem and provide a more informed basis for effective policy solutions. While some governments may fail to report incidents of which they are aware, other nations simply do not possess the capabilities necessary to effectively regulate nuclear and other radioactive materials. If no materials in a given country are genuinely under regulatory control, it is equally impossible to monitor and account for materials that fall out of regulatory control. Establishing and cultivating capacity building programs in countries where poor reporting stems from limited regulatory capabilities offers the most promising avenue for improving transparency globally.

Assistance provided under the auspices of UN Security Council Resolution 1540 as well as IAEA advisory services offer two potential vehicles for progress. Adopted in 2004, UNSCR 1540 requires all states to support efforts to prevent non-state actors from developing, acquiring, manufacturing, possessing, transporting, transferring, or using nuclear, chemical, or biological weapons and their delivery systems. All states are required to establish appropriate controls to prevent the illicit trafficking of materials and components usable in such weapons. Through the 1540 Committee, major supporters of the resolution, including the United States, the European Union, and Japan, provide education, training, and other capacity-building assistance to states that request help improving their capabilities to comply with UNSCR 1540.

The IAEA offers several services upon request from member states to help them improve regulatory controls governing nuclear and radiological security. The International Nuclear Security Advisory Service (INSServ) program allows states to work with the IAEA on drafting plans for nuclear security improvements and provides assistance to "protect against nuclear terrorism and identify ways to improve a broad spectrum of nuclear security activities."[16] Recommended topics include "the legislative and regulatory system related to nuclear security; physical protection of nuclear and radioactive material; detection of and response to illicit trafficking in nuclear and radioactive material; and human resources development in nuclear security."[17] These findings and recommendations can then be used to develop an Integrated Nuclear Security Support Plan (INSSP) tailored to country-specific needs and providing "a platform for nuclear security work to be implemented over a period of time, thus ensuring sustainability."[18]

While such programs can improve reporting in countries with limited regulatory capabilities, addressing some countries' reluctance to report known incidents to the public presents a separate and more difficult challenge. In countries where cultural reluctance or media censorship inhibit transparency, measures aimed at encouraging greater transparency or capacity building are unlikely to change reporting dynamics. Some countries may refrain from reporting incidents openly given the public's poor understanding of the health effects of radiation. This lack of understanding leads to "radiophobia," and some governments may feel increased transparency is not worth the public relations difficulty generated by headlines of lost or stolen radioactive material.[19] Efforts to educate both civil servants and the general public about the nature of radioactive materials and their associated risks may help reduce these concerns, enabling some governments to display greater transparency.

---

[16] "International Nuclear Security Advisory Service (INSServ)," International Atomic Energy Agency, http://www-ns.iaea.org/security/insserv.asp?s=4&l=26.
[17] "International Nuclear Security Advisory Service (INSServ)," International Atomic Energy Agency, http://www-ns.iaea.org/security/insserv.asp?s=4&l=26.
[18] "Integrated Nuclear Security Support Plan (INSSP)," International Atomic Energy Agency, http://www-ns.iaea.org/security/inssp.asp?s=4.
[19] The term "radiophobia" comes from Igor Khripunov (ed.), *The Human Dimension of Security For Radioactive Sources: From Awareness to Culture*, (Athens, GA: Center for International Trade and Security, University of Georgia, Indonesia's National Nuclear Energy Agency, 2014), p. 7, http://cits.uga.edu/uploads/documents/radreport.pdf.

Key Finding 2: Thieves, Smugglers, and Illicit Trafficking

Many analysts have long recognized the possibility that terrorists could link up with purveyors of illicitly acquired nuclear or other radioactive material. While there is scant evidence of an existing nexus between radioactive material trafficking and terrorism, a closer look at the capabilities and motivations of the actors involved in reported cases of theft and smuggling—along with their areas of operation—can help determine whether such a convergence could one day emerge.

Since the CNS database tracks both intentional and unintentional acts, a great many incidents captured in the dataset have seemingly no connection to criminal activity. Indeed, spotlighting genuinely illicit incidents within the larger phenomenon of out of control material reveals that, among the over 300 reported incidents, there are only 96 incidents of theft or unauthorized possession. Perpetrators were only apprehended or otherwise identified in a relatively small number, about 21 percent, of these cases. Nearly all of these individuals were supply-side actors, such as thieves or intermediaries, rather than end-users.

Thefts and Thieves

Thieves can take the form of insiders, such as employees at source facilities and licensees or custodians of radioactive sources, or outsiders with no prior affiliation with the material. Insider thieves with their direct access and knowledge of security and accounting arrangements are particularly well-placed to steal radioactive material. Security experts have long identified insiders as one of the most difficult threats to defend against.[20] Of the 85 documented thefts, insider thieves were identified in just 4 cases captured in the database.[21] However, given their unique ability to evade detection, it is certainly possible that additional, undetected insider thefts occurred. In one case of insider theft, an engineer at a mining company in Kazakhstan stole an unspecified quantity of cesium-137 from a storehouse over two decades ago. The theft did not come to light until 2014 when he was caught in a sting operation along with two accomplices trying to sell it for $250,000 (#2014209).

Although perpetrators were rarely identified, the circumstances surrounding many reported thefts indicates a majority of them were crimes of opportunity carried out by outsiders who likely did not know what they were stealing or did not specifically target a radioactive source. In a host of cases, a stolen source was found a few days later either intact or still locked inside its transport container, indicating only fleeting interest in the stolen goods. In 9 reported thefts, perpetrators stole a vehicle and were probably unaware of its radioactive contents. Still other cases involved thieves breaking into a storage area and stealing a variety of construction tools as well as devices containing radioactive sources, indicating their theft was likely coincidental. In all, 65 percent of all recovered items were found in a ditch, dumpster, or discarded in a similar manner.

Smuggling and Intermediaries

Likely intermediaries attempting to sell or transport radioactive material were identified in 17 incidents recorded in the database. In 3 cases, individuals were caught in an attempted sale of radioactive material as a result of a sting operation.[22] Another 8 cases were detected during the transportation of the material, typically at a border crossing or as the by-product of a traffic stop.[23] In the remaining 6 cases, law enforcement authorities seized material from a suspect's home or place of business, most often following an anonymous tip or prolonged investigation.[24]

---

[20] National Nuclear Security Administration, "Insider Threat to Nuclear and Radiological Materials: Fact Sheet," March 23, 2012, http://www.nnsa.energy.gov/mediaroom/factsheets/insider-threat; Matthew Bunn and Scott D. Sagan, *A Worst Practices Guide to Insider Threats: Lessons from Past Mistakes*, (Cambridge, MA: American Academy of Arts and Sciences, 2014), http://cisac.fsi.stanford.edu/sites/default/files/insiderThreats.pdf.
[21] See Incident #2013034, #2014209, #2014250, and #2014306.
[22] See Incident #2013089, #2013138, and #2014209.
[23] See Incident #2012145, #2013005, #2013011, #2013045, #2013055, #2014185, #2014280, and #2014293.
[24] See Incident #2013034, #2013088, #2013089, #2013189, #2014191, and #2014330.

Analysts have pointed to the variety of actors that fall into this category, "ranging from amateurish fortune-seekers and primitive criminals to metal-trading companies and organize crime groups."[25] In the CNS database, intermediaries were typically unsophisticated with only elementary knowledge of radioactive materials and probably minimal experience in smuggling contraband. Most intermediaries operated as individuals or in small, semi-organized groups. Only one incident (#2014330) clearly involved an organized criminal group, which operated out of Moldova and was described by law enforcement officials as having "specialized knowledge of radioactive materials." The arrest of several of the group's members, along with the seizure of material worth an estimated 1.6 million euros, was possible only through close coordination and intelligence sharing between Moldovan authorities, Interpol, and the FBI.

Organized criminal groups are clearly the most unsettling type of intermediary because they are better positioned to connect sellers and buyers and have knowledge of how to evade law enforcement.[26] The data suggest their involvement in radioactive material trafficking is limited, but given their skillset and experience, it is certainly possible such groups have largely evaded detection and are thus more involved than has been observed to date.

End-Users

Few reports allow easy identification of end-users. Among those where identification was possible, only one case involved actors with a confirmed interest in using radioactive material for malicious purposes (#2013053). In January 2013, an army patrol in the northeastern state of Assam, India discovered an improvised explosive device underneath a police station containing 1.5 kg of uranium in an unknown form. The device was reportedly linked to a rebel group known as the UFLA, which had issued a series of threats to carry out bombings prior to the device's discovery. In several other unrelated cases, reports speculated about the possible motivations of the perpetrators, but there is no proof that any of them intended to carry out an act of terrorism or otherwise intended to use the material to cause harm.

The dearth of incidents involving end-users is common to all databases.[27] Traffickers are almost always caught while looking for a potential buyer or in route to a final destination. Investigations into an incident usually stop once a suspect is apprehended, and seldom lead to information on the origin of the material or where it was headed—whether due to resource limitations, lack of will, or political barriers to information sharing. Yet, the absence of evidence is not evidence of absence. Once material ends up in the hands of end-users—whether it be proliferating states, terrorist or other extremist groups, malicious individuals, or commercial entities—there is little chance that their activities will be revealed to law enforcement. Several terrorists groups have demonstrated a clear interest in acquiring nuclear or other radioactive materials.[28] The absence of documented cases where the material has moved from supplier to black-market sellers, and buyers to malicious end-user, should not lead us to assume such incidents have not occurred in the past or will not occur in the future.

---

[25] Lyudmila Zaitseva, "Nuclear Trafficking: 20 years in Review," Paper Presentation, World Federation of Scientists, Erice, Sicily, August 2010.
[26] Lyudmila Zaitseva and Kevin Hand, "Nuclear Smuggling Chains: Suppliers, Intermediaries, and End-Users," *American Behavioral Scientist* 46, No. 6, (February 2003), p. 822-844.
[27] Lyudmila Zaitseva, "Nuclear Trafficking: 20 years in Review," Paper Presentation, World Federation of Scientists, Erice, Sicily, August 2010.
[28] James Clapper, Director of National Intelligence, "Statement for the Record on the Worldwide Threat Assessment of the U.S. Intelligence Community for the Senate Committee on Armed Services," March 10, 2011, p. 4, http://www.au.af.mil/au/awc/awcgate/dni/threat_assessment_10feb11.pdf; Jonathan Medalia, "'Dirty Bombs': Technical Background, Attack Prevention and Response, Issues for Congress," Congressional Research Service, June 24, 2011, http://fas.org/sgp/crs/nuke/R41890.pdf; Charles D. Ferguson and William C. Potter, *The Four Faces of Nuclear Terrorism*, (Monterey, CA: Center for Nonproliferation Studies, Monterey Institute of International Studies, 2004).

Policy Implication 2: Strengthening Capabilities to Detect, Disrupt, and Deter Illicit Trafficking

As former U.S. Senator and NTI Co-Chairman and CEO Sam Nunn highlights, "We know that acquiring a weapon or the [necessary] material to make one is the hardest step for terrorists to take and the easiest step for us to stop. By contrast, every subsequent step in the process—building the bomb, transporting it, and detonating it—is easier for the terrorists to take and harder for us to stop."[29] Yet, security systems can never provide absolute assurance against theft, and some material is already outside regulatory control and therefore potentially available to terrorists. Thus, while preventing loss of control is rightly considered the most effective way to combat nuclear or radiological terrorism, other steps beyond on-site security should be taken to block the full range of potential terrorist pathways to the bomb.[30]

First, given limited resources, governments that provide relevant assistance should target regions where radioactive material smuggling presents the greatest risk. Although incidents of theft, unauthorized possession, and illegal sale occur worldwide, a closer look at the CNS dataset reveals that in most regions, such events are sporadic with few common characteristics. Patterns that might indicate the existence of a genuine, although supply-side dominated, "black market" for radioactive material were only readily apparent in Eastern Europe and Eurasia. Most of the incidents occurring in these regions involved traffickers aware of the radioactive contents of their contraband and attracted to the perceived value of selling it. Experts operating with larger datasets have likewise identified the threat emanating from these regions, with one analysis pinpointing particularly worrisome trends to the area surrounding the Black Sea.[31]

Efforts to combat illicit trafficking have long focused on the former Soviet Union, and Central Asia and the Caucasus in particular, but more could be done. Unfortunately, recent developments do not paint a positive picture. Cutbacks to relevant U.S. programs in the Obama administration's latest budget request will likely slow progress.[32] In addition, the rapid decline of U.S.-Russia relations precipitated by the crisis in Ukraine will undoubtedly inhibit intelligence sharing and the development of joint projects to counter radioactive material smuggling in countries within the region and around the world. Given the deteriorating security situation in Ukraine and ongoing instability in the Middle East, these regions will likely provide fertile ground for illicit traffickers. It is thus imperative that the United States and Russia, along with regional partners, find ways to cooperate on these trafficking issues of mutual interest.

Second, cooperative programs to detect and interdict illicit trafficking should emphasize the tools that have proven most effective. As the incident data demonstrates, successful seizures of stolen or otherwise illegally held material most often resulted from traditional law enforcement and intelligence operations combined with timely tips from informants or the general public, not on radiation monitoring equipment. Radiation detectors proved most effective at detecting the inadvertent movement or improper disposal of radioactive materials rather than in catching real traffickers red-handed. A recent reassessment and two-thirds spending reduction

[29] Sam Nunn, "Ten years of reducing nuclear dangers," *The Hill*, June 3, 2014, http://thehill.com/opinion/op-ed/207915-ten-years-of-reducing-global-nuclear-dangers.
[30] Matthew Bunn, *Securing the Bomb 2010: Securing all Nuclear Materials in Four Years* (Cambridge, MA: Project on Managing the Atom, Harvard University, and the Nuclear Threat Initiative, 2010), p. 8, http://www.nti.org/analysis/reports/securing-bomb-2010/.
[31] Lyudmila Zaitseva and Friedrich Steinhäusler, "Nuclear Trafficking Issues in the Black Sea Region," *EU Non-Proliferation Consortium Papers*, No. 39, April 2014, p. 4, www.sipri.org.
[32] See NTI Securing the Bomb Interactive Budget Database, http://nukesecuritybudgets.nti.org/; Matthew Bunn, Nicholas Roth, and William H. Tobey, *Cutting Too Deep: The Obama Administration's Proposals for Nuclear Security Spending Reductions*, (Cambridge, MA: The Project on Managing the Atom, Belfer Center for Science and International Affairs, Harvard University, July 2014), http://belfercenter.ksg.harvard.edu/files/budgetpaper%20WEB.pdf.

to the U.S. Second Line of Defense (SLD) program—one of several U.S. projects that work to provide radiation detectors and relevant training to monitor key ports and border crossings worldwide—was likely justified in light of the incident data as well as "concerns in a number of quarters about the scope, cost, and effectiveness of the effort."[33] Unfortunately, it is unlikely that these funds will be re-directed towards other programs focused on building global capacity to interdict illicit smuggling that emphasize more effective tools.[34]

Finally, countries should ensure that governments around the world have strong legal frameworks in place to criminalize and effectively prosecute any individuals involved in the theft or smuggling of radioactive materials. Several international instruments require member states to adopt national laws which criminalize and set appropriate penalties for certain trafficking activities—namely the Convention on the Physical Protection of Nuclear Material (CPPNM) and its 2005 Amendment, the International Convention on the Suppression of Acts of Nuclear Terrorism (ICSANT), and UNSCR 1540. Yet application of these instruments has been uneven at best. Potential or levied sentences for those charged or convicted of holding, transporting, or selling material were referenced in only 7 cases.[35] Prison terms typically ranged from 4-10 years. In one case, a suspect faced up to 20 years behind bars.[36] The risk of capture and prosecution would likely do little to dissuade terrorists from stealing, buying, or using radioactive materials; but since the expectation of profit appeared to motivate many traffickers identified in the database, it is reasonable to assume that strong penalties could serve as a deterrent in these cases.

Several incidents captured in the CNS dataset highlight the issues surrounding burden of proof as well as intra- and inter-state trafficking. Indeed, authorities often alleged individuals apprehended while carrying material were seeking a buyer or intended to use the material for some illicit purpose, but determining their actual motivations was largely guesswork. In addition, in only 4 of 17 cases of suspected smuggling, was a suspect stopped at a border crossing, generating clear linkages to trans-boundary activity. While several cases involved the apprehension of foreign nationals, details on the origin of the material or where suspects acquired it was either unknown to or not reported by relevant authorities. To effectively prosecute trafficking cases, states may need to draft implementing legislation for relevant international instruments in such a way that accounts for these potential loopholes.

[33] Matthew Bunn, Nicholas Roth, and William H. Tobey, *Cutting Too Deep: The Obama Administration's Proposals for Nuclear Security Spending Reductions*, (Cambridge, MA: The Project on Managing the Atom, Belfer Center for Science and International Affairs, Harvard University, July 2014), p. 24-25; For an assessment of the technical limitations of radiation detectors, see Jonathan Medalia, "Detection of Nuclear Weapons and Materials: Science, Technologies, and Observations," Congressional Research Service, June 4, 2010, https://www.fas.org/sgp/crs/nuke/R40154.pdf.
[34] Matthew Bunn, Nicholas Roth, and William H. Tobey, *Cutting Too Deep: The Obama Administration's Proposals for Nuclear Security Spending Reductions*, (Cambridge, MA: The Project on Managing the Atom, Belfer Center for Science and International Affairs, Harvard University, July 2014), p. 24-25.
[35] See Incident #2013039, #2013040, #2013088, #2013089, #2013138, #2014209, and #2014280.
[36] See Incident #2013138, note this suspect was charged under U.S. sanctions laws targeting Iran's nuclear program and not under those related to the unauthorized possession of radioactive material, see U.S. Attorney's Office for the Southern District of Florida, "Individual Charged With Brokering Uranium Deal Intended For Supply To Iran," Press Release, August 22, 2013, http://www.justice.gov/usao/fls/PressReleases/2013/130822-02.html.

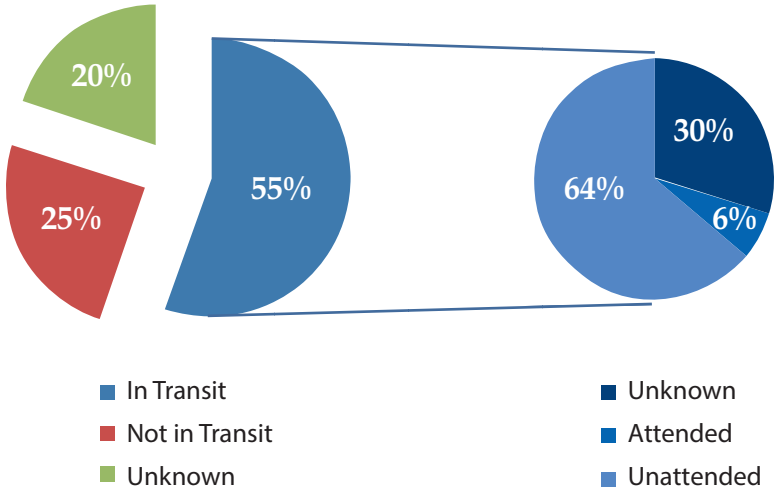
Key Finding 3: Transport and Physical Security Vulnerabilities

Although no recorded incident led directly to an immediate threat of nuclear or radiological terrorism, the circumstances surrounding any theft of radioactive materials can illuminate vulnerabilities in existing security controls. Understanding these vulnerabilities can enable policymakers to take corrective actions to prevent more serious diversion of materials in the future.

To identify the circumstances surrounding stolen radioactive material, the CNS database classifies thefts into two additional sub-categories. The first indicates the location of the material, and includes "theft from fixed site" (20 incidents); "theft from individual" (2 incidents); "theft from vehicle" (37 incidents); "theft with vehicle" (8 incidents); or "unknown" (17 incidents). The second indicates whether the material was "attended" (41 incidents) or "unattended" (3 incidents) when the theft occurred.

As identified in last year's report, the dataset suggests materials are particularly vulnerable during transport. Nearly half of all documented incidents in 2014 involved material in transit, up from nearly one-third in 2013. Of the 85 thefts recorded in the database, over twice as many occurred while in transit as did from a fixed location. In over 60 percent of thefts during transit, the material had been left unattended when the theft occurred. Unsurprisingly, the majority of radioactive sources stolen or lost during transit are contained within small, portable devices such as radiography cameras (typically Category 2 sources) and moisture density gauges (typically Category 3 and below). These devices are commonly used at temporary job sites, requiring frequent travel on the part of their operators to transport them to and from designated storage locations.

Figure 5. Thefts in Transit



Good security involves not only measures to prevent material from falling out of control, but also detection and response mechanisms that help re-establish control in the event that preventive measures fail. The IAEA notes that recovery rates for high-risk radioactive sources are typically high given concerted efforts to recover them.[37] In the CNS database, recoveries were reported in 13 of the 17 incidents involving Category 1 or 2 sources. For lower category sources, only about 40 percent of incidents involving loss, theft, or delivery failure were reported as recovered.

[37] International Atomic Energy Agency, "IAEA Incident and Trafficking Database (ITDB)," Fact Sheet, 2014, www.iaea.org.

Recovery rates should not be taken out of context. Recoveries are not often reported unless there is substantial public interest in the incident. In addition, although reporting of materials that have fallen out of regulatory control may be mandated in some countries, reporting on whether they are recovered may be discretionary. However, recovery *methods* can illuminate a great deal. While most incident reports included information on whether licensees contacted local law enforcement to report a loss or theft, details on subsequent investigations were usually scarce. A small number of cases specified response measures such as offering a reward for the device's return and notifying local vendors to be on the lookout for individuals trying to sell stolen items. In cases where details on the recovery process were provided, it appears most relied heavily on manual searches, anonymous tips, and a fair amount of luck.

For example, when a 50-60 kilogram container of cesium-137 fell off the back of a truck in Kazakhstan, it was only recovered after a taxi driver tipped off authorities (#2014281). The taxi driver, having seen a public service announcement regarding the missing material, recalled a recent passenger who had mentioned hitching a ride on a truck, the driver of which had found a container roughly fitting the description detailed in announcement. This random tip relayed through three individuals—rather than a nearly week long official search centered some one thousand kilometers away from where the material was ultimately recovered—allowed authorities to locate the container within a day.

Policy Implication 3: Strengthening On-Site and Transport Security

Thanks to the efforts of several countries to raise the profile of radiological security within the Nuclear Security Summit context, the international community has paid increasing attention to the issue in recent years. Yet there are still no international instruments that set enforceable standards for how secure radioactive materials should be. The IAEA offers non-binding guidance, but states are under no obligation to follow its recommendations. As a result, national regulations governing the security of radioactive materials vary widely.

In most countries, once a radioactive source is licensed for use, there appears to be little regulation governing its transportation and storage (this is particularly true of Category 3, 4, and 5 sources). To be sure, some interested countries have taken steps to strengthen regulations. In the United States, the Nuclear Regulatory Commission published a set of rules in 2013 governing the "Physical Security of Category 1 and Category 2 Quantities of Radioactive Material," which codifies and builds upon various orders and guidance issued since 2005.[38] The new regulations require licensees, inter alia, to institute background checks for employees granted unescorted access to radioactive material, employ physical barriers and monitoring equipment to prevent and detect unauthorized access, follow certain transport procedures, and have a response plan in place with local law enforcement in the event a theft does occur.[39]

Many stakeholders believe the new NRC regulations provide sufficient protection.[40] To be sure, thefts and losses of Category 1 and 2 sources seldom occur, and most incidents captured in the database resulted from a failure to follow regulations rather than a failure of the regulations to prevent loss of control (see next section on human negligence). While at face value this might indicate existing controls are largely effective when applied, this is not necessarily the case.

---

[38] Nuclear Regulatory Commission (NRC), 10 *CFR Part 37—Physical Protection of Category 1 and Category 2 Quantities of Radioactive Material*, March 19, 2013, www.nrc.gov.
[39] Jonathan Medalia, "Nuclear Regulatory Commission 10 C.F.R. 37, A New Rule to Protect Radioactive Material: Background, Summary, Views from the Field," Congressional Research Service, December 14, 2012, https://www.fas.org/sgp/crs/nuke/R42868.pdf.
[40] Tom Bielefeld, "Mexico's stolen radiation source: it could happen here," *Bulletin of the Atomic Scientists*, January 23, 2014, http://thebulletin.org/mexico%E2%80%99s-stolen-radiation-source-it-could-happen-here; Jonathan Medalia, "Nuclear Regulatory Commission 10 C.F.R. 37, A New Rule to Protect Radioactive Material: Background, Summary, Views from the Field," Congressional Research Service, December 14, 2012.

A host of thefts of small, mobile Category 3 and below sources occurred in transit despite the apparent application of security measures required for higher category sources. The new NRC regulations specify that mobile devices employing Category 1 and 2 sources must be secured during transit with "two independent physical controls," such as lock or chain; and if the licensee must leave a device unattended in a vehicle, the vehicle must be disabled by means other than "the removal of an ignition key."[41] In one incident, a nuclear density gauge containing a radium-226 source was stolen from a parked vehicle in Indiana despite being secured in the back of the vehicle with three padlocks and a chain (#2014225). In another case (#2014282), a moisture density gauge containing a cesium-137 source was stolen from a locked vehicle in Brooklyn even though its case (which was also locked) was "tethered to the frame of the vehicle with the cable locked to the hasp of the carrying case." These incidents along with similar examples from the larger dataset suggest the possible need for strengthened regulation of sources in transit, such as requiring that sources not be left unattended for lengthy periods in areas where there is general public access.

The need to improve detection and recovery efforts for radioactive sources has not gone unnoticed. In 2007, Washington State petitioned the NRC to consider requiring licensees to equip vehicles carrying high-risk mobile sources with GPS tracking.[42] The NRC denied the petition, claiming GPS was "neither justified nor necessary," and noting a GPS-equipped vehicle (as opposed to a GPS-equipped device) does not ensure the source will be found.[43] The CNS dataset indicates sources are more often stolen from a vehicle (41) rather than with a vehicle (3), which lends support to the NRC's decision but also points to the potential benefit of tracking radioactive sources directly.

One feasibility study commissioned in 2011 by the Department of Homeland Security and conducted at Sandia National Laboratories concluded that it is possible to tag some portable radiography and oil well logging devices, but "due to many technological hurdles, tagging and tracking of the source was not feasible with then commercially available technology."[44] South Korea already employs its own Radiation Source Location Tracking (RADLOT) system, which reportedly provides "real-time tracking" for some 1,400 sources.[45] At the 2012 Nuclear Security Summit, South Korea announced a pilot project to install the system in Vietnam with assistance from the IAEA, and agreed to share its findings with the international community once the project is complete.[46] The U.S. National Nuclear Security Administration (NNSA), in collaboration with industry partners, is also developing technology for tracking mobile radioactive sources.[47] If successful, NNSA hopes it will be ready for commercial manufacture by summer 2015. Although an assessment of the technical and cost effectiveness of these technologies is beyond the scope of this report, the CNS incident data certainly point to their potential value in recovering lost or stolen radioactive sources, and give reason to support continued investment and information sharing between such projects.

---

[41] Nuclear Regulatory Commission (NRC), "37.53 Requirements for mobile devices," in *NRC Regulations: Title 10, Code of Federal Regulations*.
[42] Government Accountability Office (GAO), *Nuclear Nonproliferation: Additional Actions Needed to Increase the Security of U.S. Industrial Radiological Source*, GAO-14-293, June 2014, p. 19.
[43] Nuclear Regulatory Commission (NRC), "Physical Protection of Byproduct Material: Final Rule," *Federal Registrar*, Vol. 78, No. 53, March 19, 2013, p. 16924, http://www.gpo.gov/fdsys/pkg/FR-2013-03-19/pdf/2013-05895.pdf; Government Accountability Office (GAO), *Nuclear Nonproliferation: Additional Actions Needed to Increase the Security of U.S. Industrial Radiological Source*, GAO-14-293, June 2014, p. 20.
[44] Nuclear Regulatory Commission, "The 2014 Radiation Source Protection and Security Task Force Report," August 14, 2014, p. 20-21, http://www.nrc.gov/security/byproduct/2014-task-force-report.pdf; Government Accountability Office (GAO), *Nuclear Nonproliferation: Additional Actions Needed to Increase the Security of U.S. Industrial Radiological Source*, GAO-14-293, June 2014, p. 37.
[45] "Republic of Korea, Vietnam, IAEA to pilot radioactive source tracking system," Nuclear Security Summit, Seoul, 2012.
[46] "Republic of Korea, Vietnam, IAEA to pilot radioactive source tracking system," Nuclear Security Summit, Seoul, 2012; Tanya Ogilvie-White, "FMWG Quarterly Regional Report for Jan-Apr 2014," Fissile Materials Working Group, http://www.fmwg.org/rr_qrs/TO-W_FMWG_Quarterly_Regional_Report_Jan-Apr.pdf.
[47] Government Accountability Office (GAO), *Nuclear Nonproliferation: Additional Actions Needed to Increase the Security of U.S. Industrial Radiological Source*, GAO-14-293, June 2014, p. 35.

Key Finding 4: Human Negligence

Half of incidents captured in the database resulted from human negligence. In 2014, 54 percent of the reported incidents were linked to negligence, including 98 percent of the 54 losses. Last year, negligence contributed to 53 percent of reported cases, including all but one of the 74 losses.[48]

Most, if not all, of the reported losses could have been prevented had relevant individuals taken greater precautions. For example, on November 12, 2014 in Channelview, Texas, a licensee of an industrial radiography camera containing a Category 2 iridium-192 source left the device on the tailgate of his truck, forgetting to properly secure it inside the vehicle (#2014287). The device fell out while in route to a temporary job site. A local police officer later recovered the device three miles from the licensee's storage facility. In another incident, staff members at a hospital in Rhode Island realized a Category 3 iridium-192 brachytherapy source was missing from its storage location (#2014230). An investigation later revealed front desk personnel had received a package containing the source, but after failing to reach the two individuals authorized to sign for it and who had previously been informed of its imminent arrival, signed the receipt and moved it to an unsecure location where it remained for eleven days.

Lax inventory controls are another common form of negligence. For instance in September 2014, through inventory reconciliation at a storage location in Woburn, Massachusetts, state regulators determined that a licensee was missing eleven static eliminators, which cumulatively contained twenty-five times the lethal dose of polonium-210 (#2014261). The licensee had not notified the agency that the devices were missing as required, and reportedly has begun to implement monthly inventory checks in response to the incident.

Negligence was also identified as a contributing factor in 11 percent of reported thefts. In these cases, licensees or custodians failed to properly secure radioactive sources. For example, on November 7, 2014, a moisture density gauge—containing two less than Category 3 cesium-137 and americium-241/beryllium sources—was stolen out the back of a pickup truck in Kirkland, Washington while it was parked overnight at the user's home (#2014284). The user should have returned the gauge to a licensed storage location at the end of the day, but chose to return home instead of driving the extra hour and a half to the storage facility. In another incident, a similar gauge was stolen from a parked vehicle along with several other items in Lakewood, Colorado (#2014199). According to the official incident report, the vehicle was locked and the device was stored within a locked transport container, but "there was no secondary tangible barrier preventing unauthorized removal of the gauge." While it is impossible to determine whether these events would have occurred even if the proper security controls had been in place, it is nonetheless reasonable to assume that such negligence on the part of licensees at least facilitated access to these devices and the speed with which thefts could be carried out.

[48] Last year we reported that negligence contributed to 100 percent of the 73 reported losses. This year we I identified a 74th loss involving two Russian radioactive thermal generators (RTGs), which had not been captured by the database at the time the 2013 report was written. The circumstances behind the incident are unknown, but Russian officials believe it was likely washed out to sea.

Policy Implication 4: Addressing Negligence through Security Culture

Security systems are only as effective as the *people* who run them. Even the most expensive and high-tech security equipment will become useless if personnel leave security doors open for convenience, turn off motion detectors to avoid false alarms, or leave access codes lying around. As General Eugene Habiger, former commander of U.S. strategic nuclear forces and former "security czar" at the Department of Energy, once put it, "good security is 20 percent equipment and 80 percent culture."[49] Security culture focuses on human behavior, individuals and organizations maintain an overlapping and mutually reinforcing set of principles, attitudes, and characteristics which serve as a means to support and enhance security.[50]

The CNS dataset also suggests that often, when a loss or theft occurs due to negligence, there is little or no personnel accountability. Warnings, reprimands, and citations are rarely reported as having been given when an incident occurs, and losses due to negligence are typically categorized as accidents. To be sure, administrators will have little reason to follow the rules unless they are enforced, and chronic offenders should be penalized. However, a change in policy to issue more frequent or harsher penalties may discourage self-reporting by individuals when radioactive materials are lost or stolen. Policies should instead focus on motivating managers and their employees to want to achieve higher levels of security.

One of the simplest ways to incentivize better performance is to educate custodians of radioactive materials about the security and safety risks of a loss or theft. Indeed, studies have shown that employees are more likely to follow rules they think are important.[51] Yet, many managers and staff "remain unconvinced or oblivious to the notion that their radioactive material might be of interest to terrorists."[52] Regular threat briefings—incorporating information on terrorists groups with a demonstrated interest in carrying out nuclear and radiological attacks as well as their abilities to build an IND or RDD—would go a long way towards removing doubts about the importance of protecting the materials for which they are responsible.[53] In addition, simulated "force-on-force" exercises involving mock teams of attackers and defenders provide valuable performance tests that can reveal vulnerabilities in a security system. Such exercises can help convince managers that additional investment is in fact needed to ensure adequate security. When resources are constrained, even a low cost and simple tabletop exercise can demonstrate holes and lapses in security planning and preparations.

Although it is impossible to definitively link negligence with a lack of training, inadequate training is known to affect awareness and attentiveness. A number of studies have examined challenges to radioactive source security in the U.S. context. Some of these studies offer insights that may have wider global applicability, as addressing the human element of security is universally challenging. For example, a 2012 GAO report noted "NRC-required training is not sufficient, and personnel at hospital and medical facilities are not required to have security training, although they implement NRC requirements at their sites." The GAO cites two specific examples of Radiation Safety Officers (RSOs), one with a background as a health physicist, and the other with

[49] Matthew Bunn, Martin B. Malin, Nickolas Roth, and William H. Tobey, *Advancing Nuclear Security: Evaluating Progress and Setting New Goals*, (Cambridge, MA: Report for Project on Managing the Atom, Belfer Center for Science and International Affairs, Harvard Kennedy School), March 2014, p. 26.
[50] International Atomic Energy Agency, "Nuclear Security Culture," *IAEA Nuclear Security Series No. 7*, Implementing Guide, Vienna, 2008, p. 3, www.iaea.org.
[51] Matthew Bunn, "Incentives for Nuclear Security," *Proceedings of the 46th Annual Meeting of the Institute for Nuclear Materials Management*, Phoenix, Arizona, July 10-14, 2005, p. 2, http://belfercenter.ksg.harvard.edu/files/inmm-incentives2-05.pdf.
[52] Tom Bielefeld, "Mexico's stolen radiation source: it could happen here," *Bulletin of the Atomic Scientists*, January 23, 2014, http://thebulletin.org/mexico%E2%80%99s-stolen-radiation-source-it-could-happen-here.
[53] Matthew Bunn, "Incentives for Nuclear Security," *Proceedings of the 46th Annual Meeting of the Institute for Nuclear Materials Management*, Phoenix, Arizona, July 10-14, 2005, p. 2, http://belfercenter.ksg.harvard.edu/files/inmm-incentives2-05.pdf.

a background in construction. Both expressed doubt concerning their abilities to understand and implement security measures. Radiation Safety Officers have primary managerial responsibility for the safety and security of radioactive materials at their organizations. It is highly unlikely, if managers lack sufficient nuclear security training, that individual workers will understand the risks associated with radioactive sources employed in their fields.

In addition to increased training, best practice exchanges provide a promising vehicle for communicating information on how to secure radioactive materials effectively. The NRC recently published a best practices guide to provide licensees of radioactive sources with a "layperson's source of practical information about security."[54] While it remains to be seen whether licensees will make good use of this resource, it should at least help those with limited security experience—but who are nonetheless responsible for it—to interpret the new regulations. By definition, however, best practices draw from experience and reflect what has proven effective over time. Thus, the NRC should be encouraged to make sure the guide does not remain a static document, but is regularly updated to reflect the state-of-play and feedback from key stakeholders.

More broadly, best practice exchanges between and among relevant security practitioners can serve to elevate the level of practice above the required "floor" to comply with regulations to the far more optimal security "ceiling."[55] Sharing best practices also helps managers identify those security measures that are not only the most effective but also the most cost-effective, thus improving the likelihood that they will actually be implemented. Best practice exchanges are still a relatively new concept in the field of nuclear security, but several venues are available.[56] All licensees, custodians, and upper-level managers should be encouraged to participate in best practice exchanges, and governments should support them financially and materially.

[54] Nuclear Regulatory Commission (NRC), Office of Federal and State Materials and Environmental Management Programs, *Physical Security Best Practices for the Protection of Risk-Significant Radioactive Material*, NUREG-2166, (Washington, DC: U.S. Government Printing Office, May 2014), http://pbadupws.nrc.gov/docs/ML1415/ML14150A382.pdf; U.S. Government Accountability Office (GAO), *Nuclear Nonproliferation, Additional Actions Needed to Increase the Security of U.S. Industrial Radiological Sources*, GAO-14-293, June 2014, p. 33, http://www.gao.gov/products/GAO-14-293.

[55] Nuclear Threat Initiative, "The Strategic Vale of Best Practices for Nuclear Security," *NTI Global Dialogue on Nuclear Security Priorities*, Non-Paper Series No. 4, November 19, 2012, www.nti.org.

[56] For an overview of existing mechanisms for sharing best practices, see Nuclear Threat Initiative, "The Strategic Vale of Best Practices for Nuclear Security," *NTI Global Dialogue on Nuclear Security Priorities*, Non-Paper Series No. 4, November 19, 2012, www.nti.org.

Key Finding 5: Material Minimization

Radioactive sources are used in numerous medical and industrial applications, for which acceptable non-radioactive alternatives exist or show technical promise. Indeed, a 2008 National Academy of Sciences (NAS) report found non-radioactive replacements "exist for nearly all applications of Category 1 and 2 [radioactive] sources."[57] The CNS database includes 17 incidents involving Category 1 or 2 sources, 16 of which involved sources used in medical (4 incidents) or industrial (12 incidents) applications.[58] Among those incidents involving medical devices, two involved sources for which non-radioactive alternatives are now commercially available. For example, many hospitals in the United States and other developed countries have switched from using teletherapy devices—such as the highly-publicized Category 1 cobalt-60 source stolen outside Mexico City in December 2013—to employing linear accelerators (linacs) to deliver comparable medical treatment. Like X-ray machines, "accelerators produce radiation only when they are on, but do not contain anything radioactive and therefore pose little risk of misuse."[59] Similarly, a "Gamma Knife" that went missing in Canada in April 2013 is commonly used to treat brain lesions, a treatment which in some cases can be performed by linac-based alternatives.[60]

Radiography cameras containing iridium-192 (11 incidents) or selenium-75 (1 incident) accounted for all 12 cases involving high-risk industrial sources. These devices are typically used to inspect welds, pipelines, and other structures for safety and quality control purposes. According to the NAS study, about 75 percent of radiography inspections performed today could be performed using alternative technologies, such as x-ray or ultrasonic methods.[61] Although some companies are switching to alternatives, a shortage of personnel trained in these methods has limited the replacement rate.[62] Even so, debate remains over whether these alternatives are practical and economically viable across the industry. Moreover, given that iridium-192's short 74-day half-life makes it less suited than other materials for use in an RDD, governments may wish to focus their efforts on minimizing the use of higher risk sources used in other applications.

A 2014 report from the U.S. Radiation Source Protection and Security Task Force brings attention to the issue of replacing and minimizing the use of Category 3 sources.[63] As previously mentioned, an RDD built from a Category 3 source, although unlikely to cause fatalities, could cause significant economic disruption, and several sources could be assembled into higher category quantities of radioactive material.

Some research, including a project supported by the U.S. Department of Homeland Security, has investigated potential replacements for americium-241/beryllium sources commonly used in well-logging and moisture density gauges.[64] However, little attention has been paid to technology alternatives for Category 3 and below sources, though they account for the vast majority of incidents in the CNS database.

---

[57] National Research Council, *Radiation Source Use and Replacement: Abbreviated Version*, (Washington, DC: The National Academies Press, 2008), p. 171.
[58] In one outlier case, the incident report included insufficient information to determine the type of device involved. The second outlier involved a radioisotope thermoelectric generator (RTG) used to generate electricity in remote locations, which in this case was used to power a lighthouse in the Artic.
[59] George M. Moore and Miles A. Pomper, "Lessons from a Mexico Theft," *Bulletin of the Atomic Scientists*, December 12, 2013, http://thebulletin.org/lessons-mexican-theft.
[60] National Research Council, *Radiation Source Use and Replacement: Abbreviated Version*, (Washington, DC: The National Academies Press, 2008), p. 177.
[61] National Research Council, *Radiation Source Use and Replacement: Abbreviated Version*, (Washington, DC: The National Academies Press, 2008), p. 145.
[62] National Research Council, *Radiation Source Use and Replacement: Abbreviated Version*, (Washington, DC: The National Academies Press, 2008), p. 135.
[63] Nuclear Regulatory Commission (NRC), "The 2014 Radiation Source Protection and Security Task Force Report," August 14, 2014, p. 45, http://www.nrc.gov/security/byproduct/2014-task-force-report.pdf.
[64] Nuclear Regulatory Commission (NRC), "The 2014 Radiation Source Protection and Security Task Force Report," August 14, 2014, p. 46, http://www.nrc.gov/security/byproduct/2014-task-force-report.pdf.

Policy Implication 5: Studying and Promoting Conversion Opportunities

One of the most effective ways to reduce the likelihood of terrorists acquiring the necessary materials to build a nuclear or radiological weapon is to minimize the number of places where they can find it. Minimizing the civilian use of weapons-usable *nuclear* material has been a central focus of the international nuclear security agenda. Far less priority has been given to radioactive source minimization and replacement, although support has grown in both the United States and abroad in recent years.

Notably, at the 2014 Nuclear Security Summit the United States committed to establishing "an international research effort on the feasibility of replacing high-activity radiological sources with non-isotopic replacement technologies, with the goal of producing a global alternative by 2016."[65] Following up on this pledge, U.S. Secretary of Energy Ernest Moniz announced at the IAEA in September 2014 the United States had committed to a joint project with France, the Netherlands, and Germany "to establish a roadmap of actions over the next two years…to support alternatives for radioactive sources."[66] Understandably, and perhaps correctly, such efforts have focused predominantly on sources with large quantities of high-risk radioactive material. However, few incidents recorded in the database involved such sources, probably because they are typically large, and once installed, remain stationary, making loss or theft less likely while they are in use. As countries afford greater priority to developing alternatives, it may be worthwhile to place increased emphasis on examining substitutes for smaller, more portable, and readily concealed sources given their greater susceptibility to loss or theft.

Regardless of the types of sources such efforts prioritize, they will only be successful if the technology alternatives are commercially viable. Despite the fact many substitutes have proven technically feasible, industry has been slow to embrace them because "the price of [radioactive] sources is often lower than that of non-[radioactive] alternatives."[67] One reason for this differential is that licensees and manufacturers in many countries are often not required to pay the full life-cycle costs, including disposal costs, of certain sources, which passes the burden on to the public.[68] Indeed, a number of incidents captured in the database appear to have resulted from improper disposal of a device containing a radioactive source. This is partly because there is no commercial disposal pathway available for certain sources, forcing end-users to keep them in storage and creating risks of improper source disposal. The IAEA and others have forwarded several options for developing viable disposal and recycling pathways, but as one expert notes, "the critical problem is political in nature…publics do not want waste disposal sites near their neighborhoods."[69]

Another explanation for the comparative advantage enjoyed by radioactive sources results from the fact "the price a user pays does not accurately incorporate the economic risks of damage to incomes and property should a terrorist radiological attack occur."[70] One expert study recommends improving liability and insurance regimes governing radioactive sources in order to incentivize users either to switch to non-radioactive alternatives or adopt stronger security controls. [71]

---

[65] "National Progress Report: United States of America," Nuclear Security Summit 2014, The Hague, March 24-25, 2014, https://www.nss2014.com/sites/default/files/documents/united_states_of_america.pdf.
[66] Ernest Moniz, "2014 IAEA General Conference Remarks as Prepared for Delivery," 58th IAEA General Conference, Vienna, September 22-26, 2014, http://www.iaea.org/About/Policy/GC/GC58/Statements/usa.pdf.
[67] Miles A. Pomper, *Mind the Gap: The Role of Liability and Insurance Regimes in Strengthening Radiological Security*, (Monterey, CA: Center for Nonproliferation Studies, August 2014), p. 1, http://www.nonproliferation.org/mind-the-gap/.
[68] National Research Council, *Radiation Source Use and Replacement: Abbreviated Version*, (Washington, DC: The National Academies Press, 2008), p. 172.
[69] Charles Ferguson, "Ensuring the Security of Radioactive Sources: National and Global Responsibilities," USKI Working Paper Series, US-Korea Institute at SAIS, March 2012, p. 21, www.fas.org.
[70] Miles A. Pomper, *Mind the Gap: The Role of Liability and Insurance Regimes in Strengthening Radiological Security*, (Monterey, CA: Center for Nonproliferation Studies, August 2014), p. 1, http://www.nonproliferation.org/mind-the-gap/.
[71] Miles A. Pomper, *Mind the Gap: The Role of Liability and Insurance Regimes in Strengthening Radiological Security*,

Converting new production to non-radioactive alternatives—when this is warranted—will reduce the overall costs of life-cycle management of radioactive sources as well as the risks of radiological terrorism. However, conversion efforts should specifically provide for the safe, secure, and comprehensive disposal of obsolete sources. Otherwise, they risk precipitating improper disposal of any devices containing obsolete sources, worsening associated safety and security challenges. As greater attention is given to radioactive source minimization and replacement, governments should perform comprehensive cost-benefit analyses of select cases to determine if conversion is warranted, and prepare to offer assistance to encourage suppliers to move to alternative technologies and dispose of obsolete sources.

(Monterey, CA: Center for Nonproliferation Studies, August 2014) http://www.nonproliferation.org/mind-the-gap/.

IV. Conclusion

The potential link between nuclear trafficking and terrorism is still seen by many experts as the number one security threat facing countries around the world. While the open source reporting captured in the CNS Global Incidents and Trafficking Database shows that this threat is still remote, there is still the obvious problem of incomplete data. Do these reports represent the norm, or are the few fissile material cases reported in 2014 simply the tip of a larger, and profoundly dangerous, iceberg?

Fortunately, there is no need to wait to find out. A close look at the data trends over the past two years shows several policy actions that are both uncontroversial and relatively easy to implement. All of them would make it harder for terrorists to acquire radioactive or fissile materials as well as provide governments and researchers with more complete information about the scope of the problem.

Acquiring better data is the first step. As reported in key finding 1, only five countries (Australia, Belgium, Canada, France, and the United States) currently make official regulatory incident reports available to the public on a regular basis. In most countries of the world, incidents typically come to light after being reported by the media. This leads to inconsistency in reporting as some journalists may not understand or accurately report the incident. It also undermines the role of government regulatory bodies because it encourages the sense that the government is either unable to report on incidents, or unwilling to do so. States that sponsor training and awareness programs related to nuclear trafficking should encourage partner nation regulatory bodies to publish incident information. The fact that five nations already routinely do so is proof the risk is low, and the public benefit both in trust and prevention of future incidents is obvious.

There is mounting evidence that radiological materials are often stolen for a simple profit motive. While the connection between thieves and terrorists has thus far been tenuous, law enforcement must remain vigilant. Crime networks are broad and frequently cross borders, and the profit motive means criminals are always seeking new customers. For this reason, law enforcement awareness of the terrorism risks of radiological materials should be increased. Regional cooperation to pool intelligence and operational resources should also be encouraged. Finally, continuing to develop laws to prosecute illegal possession of radiological or nuclear materials and strengthen penalties will also help deter theft of these materials.

The incident reporting clearly shows most materials disappear from control during transport. Standardizing physical security measures as part of licensing and regulation is one part of the solution. Another improvement would be to take advantage of improvements in tracking technology to tag individual pieces of equipment. Radio frequency identification (RFID) tags and global positioning system (GPS) tracking have matured to the point that the location of most devices (if not the actual source materials) can easily be tracked in real time. Regulatory bodies should consider encouraging adoption of these technologies for users and manufacturers.

The human factor in most of the incidents reported cannot be ignored. Materials were lost or stolen because a driver failed to lock them up or a worker forgot where he left them. Awareness of the sensitivity of these materials must become a universal aspect of basic owner and operator training. Just as health and safety risks are part of radiological material licensing, security awareness should also be included.

Of course, the best way to avoid theft or loss of radiological or nuclear materials is not to use them in the first place. This does not need to be an all or nothing approach. But, regulators, manufacturers, and users should be made aware that reasonable alternatives do exist on occasion, and the opportunity to embrace these alternatives when feasible should be promoted.

The number of incidents in the CNS database continues to grow, and with them improved opportunities for analysis. By making the complete dataset available, the hope is outside researchers and the interested public will join with the nonproliferation community to uncover future indicators and trends that will help to reduce the threat of illegal nuclear trafficking.

V. Methodology

For a complete methodology and dataset, please refer to the full database at www.nti.org/trafficking.

- The database includes incidents reported January 1, 2013 through December 31, 2014
- CNS researchers conducted global searches in 13 major languages. Use of these languages also enabled in-depth native language searches for incidents in 90 countries.
- Researchers used a variety of information sources, including countries' regulatory agencies, national and local news reports, and country-specific search engines.
- The database includes twenty categories describing each incident. The categories and their subsequent subcategories are explained in the Category Definitions section of the database.

Incidents identified as linked to human negligence in Key Finding (4) are not classified as such in the database. The following guidelines were used to determine whether negligence was a contributing factor in an incident:

- Negligence was defined as a lack of reasonable care or attention to maintaining control over radioactive materials, including any failure to follow relevant regulations or company procedures governing the use, storage, shipment, receipt, or disposal of radioactive materials.
- The circumstances surrounding how material fell out of regulatory control had to be described in the incident report in order to link an incident to negligence. If insufficient details were given, the role of negligence was deemed unknown.
- All incidents classified as "loss" were deemed due to negligence unless the circumstances surrounding loss of control involved a natural disaster or other events outside the control of the individual(s) responsible, such as a health event.
- Incidents classified as "delivery failure/misrouting" were deemed due to negligence if a shipment was delivered to the wrong address or location, was labeled improperly, contained more or less material than was specified in the invoice, was the result of a communication breakdown, or relevant individuals did not otherwise follow the proper procedures for shipping, receiving, or opening radioactive materials.
- In cases classified as "theft/stolen material," the incident report had to specifically mention whether the user failed to follow relevant regulations or company protocols at the time the theft occurred.
- Cases falling into all other categories listed under "Type of Incident" were linked to negligence if the incident report mentioned activities that fit the definition of negligent behavior detailed above.