

The Security of Medical and Industrial Radioactive Sources

Tom Bielefeld^{a*}, Helmut W. Fischer^b

^aBelfer Center for Science and International Affairs, Harvard Kennedy School, 79 JFK St., Box 134, Cambridge, MA 02138, USA.

^bRadioactivity Measurements Laboratory, Institute of Environmental Physics, University of Bremen, Postfach 330 440, 28334 Bremen, Germany.

Abstract. Recent foiled and successful terrorist plots in Europe and the US (including two cases in the UK and Germany which included plans to design radiological dispersal devices in 2004 and 2005), clearly demonstrate that domestic or locally acting terrorist cells have become an important part of the terrorist threat picture. The uncovered “dirty bomb”-plots involved radioactive material of type or quantity that would not have caused much damage. Still, these observations underscore the necessity to revisit the issue of radioactive sources security in countries which may become the target of a radiological attack. This includes in particular countries in Europe, many of which in the past relied on sophisticated - but safety centred - regulations and functioning oversight institutions. In a pilot study, we have developed plausible attack scenarios involving medical and industrial sources used in Germany. Special emphasis was put on how such sources could be obtained by a locally acting terrorist group using criminal tactics and non-specialized equipment only. To this end, sources storage and handling as well as daily work procedures in hospitals and companies have been analysed to find weak points which could be discovered and exploited by terrorist groups. Publicly available technical information has been used to assess under which circumstances terrorists could obtain various types of sources or whole instruments. Calculations have been performed to estimate the radiation burden to a person handling these sources with improvised equipment. Our study shows that, even in a country with already high regulatory standards, hospitals and industrial facilities still need to introduce improvements to sources security. We therefore discuss and propose a number of affordable security upgrades. Many of our findings in Germany apply to other western countries as well. Hence, we call for a change of mentality of users and manufacturers to take into account not only the safety but also, and more thoroughly, the security aspects of the use of radioactive materials. In today’s world, sources are not only dangerous to handle, they are also themselves in danger of being used by terrorists. The once-popular notion of “self-protecting” radioactive sources no longer holds.

KEYWORDS: *terrorism; radiological dispersal device (rdd); teletherapy; irradiator; radiography; transport.*

1. Introduction

Recent foiled and successful terrorist plots in Europe and the US involving al Qaeda affiliated groups clearly demonstrate that domestic or locally acting terrorist cells have become an important part of the terrorist threat picture. The emergence of these so-called “home-grown” terrorist cells acting on behalf or in the spirit of a transnational terrorist organization which demonstrably has been seeking to acquire weapons of mass destruction is a serious cause of concern. In two of the cases, the plots uncovered involved the manufacture and use of radiological dispersal devices (RDD), or “dirty bombs”. In August 2004, British police arrested Dhiren Barot, leader of a group of eight men, which planned to carry out multiple terrorist attacks in Britain and in the United States. Among the group’s plans was setting on fire ten thousand household smoke detectors to disperse the small amounts of americium which they hold [1]. In January 2005, German police apprehended an Iraqi and a Palestinian who unsuccessfully attempted to acquire 46 grams of highly enriched uranium from a group in Luxemburg, allegedly on behalf of al Qaeda [2]. Both these plots involve radioactive materials in types or quantities that would not cause much damage if used as an RDD, but they demonstrate the interest of jihadi extremists in mounting RDD attacks. Moreover, they highlight the possibility that locally acting terrorist groups may choose a local path of acquiring radioactive materials, i.e. to get their hands on radioactive sources within the country in which they plan to attack.

* Presenting author, E-mail: Tom_Bielefeld@ksg.harvard.edu

These developments underscore the necessity to revisit the issue of radioactive sources security within the countries which may become the target of an RDD attack. This includes in particular countries in Western Europe, where, in the past, the focus of attention had been to prevent the smuggling of nuclear and radioactive materials from outside into the country. Security issues were widely being considered a problem of Eastern European states or the developing countries. With functioning oversight institutions in place, countries like Germany considered its body of regulations sufficient, even though said regulations focussed on nuclear and radiological safety rather than security.

Scenarios, in which terrorists acquire radiological materials elsewhere and attempt to smuggle them into the country in which they plan to attack remain plausible today. However, statistics concerning lost and stolen sources bear witness to the fact that control and security of radioactive sources is not only a problem of the successor states of the Soviet Union. According to an estimate by the Commission of the European Communities, about 70 radioactive sources are lost every year in its member states [3]. This means, the sources are no longer accounted for, i.e. they have been stolen, been illegally disposed of, or have otherwise been untraceable for the responsible authorities. For the US, the corresponding estimates are 300 lost sources per year [4]. Only part of them is eventually recovered, oftentimes at scrap yards. By far the most of these so-called orphaned sources do not have a large radioactive inventory. But the sheer numbers illustrate that there is the need for action.

There have been regulatory initiatives on the European level in recent years to address this problem. In Germany, these have led to new legislation for the control of highly radioactive sources and to the set up of a nationwide central register for such sources in late 2005 [5].

Regardless of these most welcome developments, questions remain about the actual state of security and protection against theft for medical and industrial sources at the facilities where these are used and stored. Could a local terrorist cell really steal a radioactive source from a hospital or a company in their neighbourhood? If yes, how difficult would it be? And finally, what needs to be done to prevent such scenarios, or to make them less likely to succeed?

The pilot study about which we report here attempted to answer these questions for the case of Germany, a country with a highly developed safety culture, with comprehensive legislation and functioning institutions overseeing facilities and enforcing the corresponding legal provisions. We believe that our study's findings may also be useful for other countries with a similar degree of regulatory authority.

2. Security Evaluation Methodology

In order to investigate the security of radioactive sources widely in use in Germany, we analysed facilities and work procedures at locations where such materials are used or stored. We located these facilities, hospitals and companies, using the internet and phone directories. We then contacted the facility managers and, upon getting permission, visited the sites. Since this was a pilot study, the number of hospitals and companies we visited was limited.¹ Also, not every company we approached was willing to collaborate with us. However, we were able to cover a variety of different types of facilities and radioactive sources. Some of the sites were local branches of companies operating nationwide, and were described to us as being representative of the companies' other facilities as well. A number of the hospitals and companies shared their experience with transport businesses with us. Moreover, some companies involved in our study themselves transport sources and source holding instruments on a regular basis. We are therefore confident that our study provides a useful survey of the security situation in Germany for sources in stationary and mobile use, and during transport.

For each facility we visited, an initial facility characterization was conducted, following the approach for physical protection evaluations developed at Sandia National Laboratories [6]. This analysis was

¹ Facility managers allowed us to conduct our study on the condition that their hospitals and companies not be identifiable. Therefore, and for obvious security reasons, we do not provide exact numbers or other information which could lead to direct or indirect identification of particular sites.

based on openly accessible information about the facility, interviews with the management and staff working with the sources, and our own observations. We call the resulting characterization “initial” because the amount of information we were able to collect varied between the different facilities. We focussed on facility operations and procedures, including employment policies, as well as on site characteristics such as building layouts, accessibility, surroundings, and existing safety and security systems. Except for compliance with safety and security regulations, we disregarded legal and liability issues. Also, we were not able to study detailed aspects of the facilities’ physical infrastructure, such as electrical power supply systems and access to the sites’ telephone and communication hubs. However, these omissions were in line with the limited scope of our study, which did not include the design of a comprehensive physical protection system for each of the facilities under investigation.

The threat definition which underlies our study is motivated by recently observed patterns of locally acting jihadist terrorist groups in Germany and Great Britain. We assumed that a facility may be attacked by an individual or a small group of people, with or without insider support. We also assumed that the attackers use ordinary criminal tactics (as opposed to a military commando-style assault), including facility observation and extortion. Attackers in our scenarios may use off-the-shelf or improvised tools and equipment and have at least a moderate technical background. Scenarios with insider support could also involve specialized equipment for source handling. Furthermore, we assumed that the attackers are motivated by extremist beliefs and may or may not be willing to accept bodily harm or to sacrifice their own health. With respect to possible health effects due to improper handling of radiation sources, we conjectured that not all potential attackers may have an accurate conception of the dangers that these sources pose.

Finally, we considered only theft scenarios, i.e. scenarios in which the attackers attempt to steal a radioactive source from the facility. Hence we did not consider scenarios in which the attackers manipulate a source to cause damage within the facility or attempt to set off an RDD in the facility itself. We also did not consider scenarios in which terrorists attempt to acquire radioactive materials by ordering them directly from a manufacturer or legitimate vendor with a counterfeit license.

The types of radioactive sources we encountered in our study consisted of IAEA safety classification I, II, III, and IV sources. They were used in teletherapy machines for tumor treatment (^{60}Co sources with a typical activity of 370 TBq)², blood and research irradiators (^{137}Cs , 100 TBq), industrial radiography (^{192}Ir , 7.4 TBq and ^{75}Se , 3 TBq), afterloading units for brachytherapy (^{192}Ir , 370 GBq), capsules for therapeutic thyroid applications (^{131}I , 5.5 GBq), and seeds for prostate brachytherapy (^{125}I , 30 MBq). These sources not only differ greatly in their radioactive inventory, they are also different from each other in their physico-chemical form, the way they are embedded in treatment or measurement instruments, and in regard to their mobility. Such factors are all important for a consequence analysis, which, accordingly, leads to a variety of different scenarios. These range from radiological attacks with negligible effect to attacks on individuals using sources of moderate radioactive inventory, and further to large scale contaminations through the explosive or non-explosive dispersal of high activity sources. In our study, we prioritize category I, II, and III sources. Such sources, either individually or on aggregate, are most likely to cause medium to high consequences in terms of casualties, public health, and socioeconomic damage.³

² Activities given in this list represent typical activities for the applications, and do not necessarily refer to the actual sources at the facilities we visited.

³ Results about our analysis of possible attack scenarios on the basis of the sources we encountered in this study will be presented elsewhere. For a preliminary summary of some of these findings, see [7].

3. Findings⁴

Both in hospitals and industrial facilities we found that staff and management exhibited a satisfactory to high level of responsibility and was well informed about the regulations concerning safety and security of the sources in use. These were, for the most part, accurately implemented in the places we visited. However, it was quite obvious that in all cases the centre of attention lay on the prevention of accidents and harm to people due to improper use of the sources. In other words, the staff we encountered focussed invariably on the safety aspects of source handling and storage. A potential risk that the sources themselves could be subject to theft by terrorists was clearly not on their minds.

This lack of security awareness is problematic especially in hospital environments. Hospitals are public spaces with a high throughput of people. Concerns about privacy prevent hospitals from the extensive use of technical security systems like video cameras, especially in treatment areas where most of the instruments with radioactive sources are located. Intrusion sensors for the off-hours are not widely in use. In some of the hospitals we visited, the policies concerning access to areas where there are radioactive sources are rendered useless by insufficiently protected access to the keys to these areas.

In companies, basic physical security measures, such as technical security systems and access controls, are implemented to provide basic protection against burglary. Intrusion detectors and video surveillance are more common. Sources which are not part of an immobile device are generally kept within their shielding containers in safes, even though a large fraction of the staff has access to these. Here, the vulnerability is highest when the source holding instruments are taken out on the road, to be used at a customer's plant or construction site, or during transit. These vulnerabilities multiply when employees, either out of negligence or in reaction to high workloads, resort to practices not in compliance with approved work procedures (such as leaving the device unattended for short periods of time).

Consequently, in almost all the facilities we visited, there appeared to be opportunities for getting access to the devices holding the sources, and for doing so without being detected. In some cases it appeared to be possible to steal the sources including their shielding containers. In most but not all of the corresponding scenarios, the theft would have been noticed within minutes to hours. Not all presumably successful theft scenarios we conceived of involved the assistance of an insider, and many did not require the coercion or application of force to security guards or staff.

The sources with the highest activities we encountered, namely those used in blood or research irradiators and teletherapy units, are embedded in fixed, immobile machines. These heavy instruments are – within our threat definition – very unlikely to be stolen. Therefore, in order to steal the sources, the irradiators and teletherapy units would have to be dismantled on the scene. There is no analysis in the public realm which answers the question how difficult it would be for potential attackers to remove a radioactive source from one of these devices, without specialized equipment.

4. “Self-Protecting” Radioactive Sources?

As this question touches upon the widespread notion of “self-protecting” radioactive sources, we attempted to investigate it further. Since we did not cooperate with manufacturers of teletherapy machines and irradiators, we resorted to a paper study. Based on the analysis of technical drawings included in service manuals and company brochures (some of them we retrieved from the internet), we drew up notional dismantling scenarios. From these we estimated a range of expected radiation

⁴ In what follows, we present our findings but withhold some technical details because we do not want to give away information which could be of use for terrorists and criminals. In publishing this study, we attempt to strike the delicate balance between informing policy makers and source users about security problems, so that these issues will be addressed, and discussing ideas that could prompt persons with malicious intent to try to steal such sources. The latter are strongly advised to carefully read the paragraphs in the following section dealing with the serious and potentially lethal consequences of improper handling of radioactive materials.

burdens for a person who attempts to remove the sources with varying sets of tools and improvised shielding measures. Naturally, there are large uncertainties associated with this approach. We therefore complemented it with an analysis of accidents and thefts involving such devices.

The picture that emerged from this analysis is a mixed one. For instance, in two well documented cases involving teletherapy units, theft attempts of parts of the devices conducted by scavengers unaware of the radiation hazards were initially successful. However, both in Goiânia (Brazil) in 1987 and in Samut Prakarn (Thailand) in 2000, further dismantling of the teletherapy unit heads without protective shielding resulted in catastrophes with numerous people dead or severely injured [8, 9].

While shielding is of utmost importance when dealing with these high activity sources, it is not a simple task to achieve. Only a few minutes of short-distance, unprotected exposure to some teletherapy sources will lead to a lethal radiation dose, with symptoms such as nausea and vomiting setting in within a very short time. Small mistakes on the part of the attacker may potentially lead to their incapacitation on the scene. Two further accidents with teletherapy machines provide instructive examples in this regard. In Sainte (France) in 1981, a technician touched a ^{60}Co source, which had fallen out of the unit head, with his unprotected hands for eleven seconds. This exposure resulted in the loss of both hands [10]. In Lima (Peru) in 1996, a mechanic approached a ^{60}Co source which had gotten stuck in a partially shielded position. His right hand was exposed to the source for only two seconds at a distance of one centimeter, still resulting in severe radiation burns and the eventual loss of two fingers [11].

The result of our analyses is that source handling poses an obstacle which appears difficult to overcome. However, the combination of the possibility of improvised shielding and some potential attackers' disregard for their own safety (or their lack of knowledge) means that even large medical or industrial sources can no longer be considered self-protecting.

5. Do Statistics Support Our Findings?

In order to put our findings into perspective, it is useful to look at actual data concerning thefts and accidental losses of radioactive sources. Useful data was available for Germany, and two other countries with a comparable level of regulatory oversight, namely Canada and the United States.

Official data on "exceptional incidents" with radioactive sources in Germany, released annually by the German Federal Ministry for the Environment lists for the years 2000 to 2005 a total of 59 losses or thefts [12]. None of these included IAEA safety category I or II sources. Only seven of the incidents were transport-related. This means in particular, that some of the sources of highest concern, namely radiography sources in transit, were not subject to theft during this time period.

This is in contrast to the situation in Canada and the US. Canadian journalists compiled a database of lost and stolen sources for the years 2002 to 2007 [13]. Of the 76 radioactive sources listed in their database, about half were subjects to theft. Sources were often "stolen from cars, disappear[ed] from construction sites, [and fell] off trucks". In the United States, the Nuclear Regulatory Commission has published data of lost and stolen category I and II sources for the time period 1994 to 2005 [14]. It reports 60 lost or stolen sources during that period, with 30% of the incidents being thefts. 57 of the lost or stolen sources were industrial radiography sources, 80% of which were eventually recovered.

The data from Canada and the US confirm our finding that the transport of sources is a weak spot in sources security. Even though the corresponding data for Germany is encouraging, it must be pointed out that its security systems for high activity sources so far have not been put to the test by terrorist groups. They seem to be working well, however, to prevent random thefts such as car thefts in which the radioactive source is not the primary target.

6. Conclusion and Recommendations

There is no doubt that the planning and execution of attacks with radiological weapons is well within the capabilities of both transnational and local terrorist groups. This refers to the illegal acquisition of radioactive materials, to the design of a weapon, and to the actual execution of an attack.

There exist some obstacles which make the preparation of a radiological attack more difficult than generally assumed. One such obstacle is the handling of highly radioactive materials, which, if done improperly or without special equipment, poses severe health risks for the attackers. However, this fact alone no longer constitutes a sufficient level of theft protection.

Our study showed that even in a country with already high standards for safety and security, hospitals and industrial facilities still need to introduce improvements in sources security. Appropriate physical protection systems include improved detection systems like video cameras and intrusion alarms. They also require systems which delay access to the sources, both to the rooms in which the sources are stored and to the machines themselves which hold the sources. In some important cases, useful detection and delay systems can be acquired and maintained at a fraction of the cost of the actual instrument to be protected. Examples of such systems are as simple as hardened doors and robust key cabinets, and include sensors, seals, and welded reinforcements at the machines.

Most importantly, the management and staff of all facilities in which radioactive materials are used and stored need to analyse their own daily work procedures and policies of who has access to which rooms, including auxiliary and cleaning staff. A two-person rule of access should be standard for all radioactive sources of IAEA safety classification category I, II, and III. Similar recommendations can be made for companies transporting radioactive materials. In some instances, especially for the sources of highest concern, it may be advisable to consider the employment of armed guards.

Relatively inexpensive but visible security improvements could also function to discourage potential attackers, who may otherwise conclude that radioactive sources are easy to steal, possibly underestimating the dangers posed by some of them.

The foundation for all of this is a considerable increase in security awareness. The need of a mentality change for users of radioactive sources was the most obvious result of our study. While there is sensitivity for the safety aspects of source handling, there is hardly any for sources security. In today's world, sources are not only dangerous to handle, they are also themselves endangered of being misused for terrorist purposes. The formerly popular notion of "self-protecting" radioactive sources no longer holds.

REFERENCES

- [1] ZAGORIN, A., E. SHANNON, E., London's Dirty Bomb Plot, Time, 3 October 2004.
- [2] Mutmaßliche Terroristen in Deutschland gefasst, Agence France Press, 23 January 2005.
- [3] COMMISSION OF THE EUROPEAN COMMUNITIES, Proposal for a Council Directive on the Control of High Activity Sealed Radioactive Sources. Brussels (2002).
- [4] INTERNATIONAL ATOMIC ENERGY AGENCY, Inadequate Control of World's Radioactive Sources, Press Release 02/09, IAEA, Vienna (2002).
- [5] COUNCIL OF THE EUROPEAN UNION, Council Directive 2003/122/Euratom of December 22, 2003; DEUTSCHER BUNDESTAG, Gesetz zur Kontrolle hochradioaktiver Strahlenquellen, August 12, 2005.
- [6] GARCIA, M. L., The Design and Evaluation of Physical Protection Systems, Butterworth-Heinemann, Boston (2001).
- [7] BIELEFELD, T. , FISCHER, H. W., Security and Damage Potential of Commercial Radioactive Sources, Journal of Nuclear Materials Management 15 3 (2007), 14-17 .

- [8] INTERNATIONAL ATOMIC ENERGY AGENCY, The Radiological Accident in Goiânia, IAEA, Vienna (1988).
- [9] INTERNATIONAL ATOMIC ENERGY AGENCY, The Radiological Accident in Samut Prakarn, IAEA, Vienna (2002).
- [10] NÉNOT, J.-C., GOURMELON, O., Les accidents dus aux rayonnements ionisants – le bilan sur un demi-siècle, L’Institut de radioprotection et de sûreté nucléaire, Clamart (2007).
- [11] KINOSHITA, A., et al., Evaluation of a high dose to a finger from a Co-60 accident, Health Physics 84 4 (2003) 477-482.
- [12] BUNDESMINISTERIUM FÜR UMWELT; NATURSCHUTZ UND REAKTORSICHERHEIT, Unterrichtung durch die Bundesregierung, Umweltradioaktivität und Strahlenbelastung im Jahr 2000 (Parlamentsbericht), and the following annual reports, http://www.bfs.de/de/bfs/druck/uus/pb_archiv.html .
- [13] BRONSKILL, J., BAILEY, S., Radioactive Devices: Dozens Lost in Canada, TheStar.com, July 3, 2007, <http://www.thestar.com/printArticle/232095> .
- [14] RADIATION SOURCE PROTECTION AND SECURITY TASK FORCE, Report to the President and the U. S. Congress Under Public Law 109-58, The Energy Policy Act of 2005 (2006).