



U.S. Department of  
**ENERGY**



# **GLOBAL THREAT REDUCTION INITIATIVE**

*Orphan Radioactive Sources and  
Threat/Vulnerability Environment*

*Presentation for End of Life Management of Radioactive  
Sources, Paris, France, September 17 and 18, 2014*

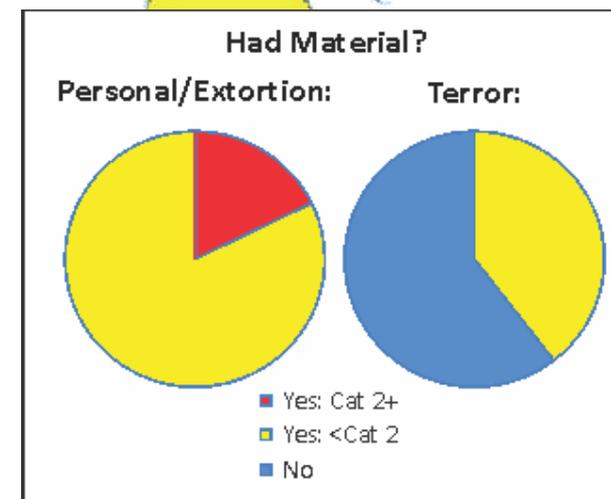
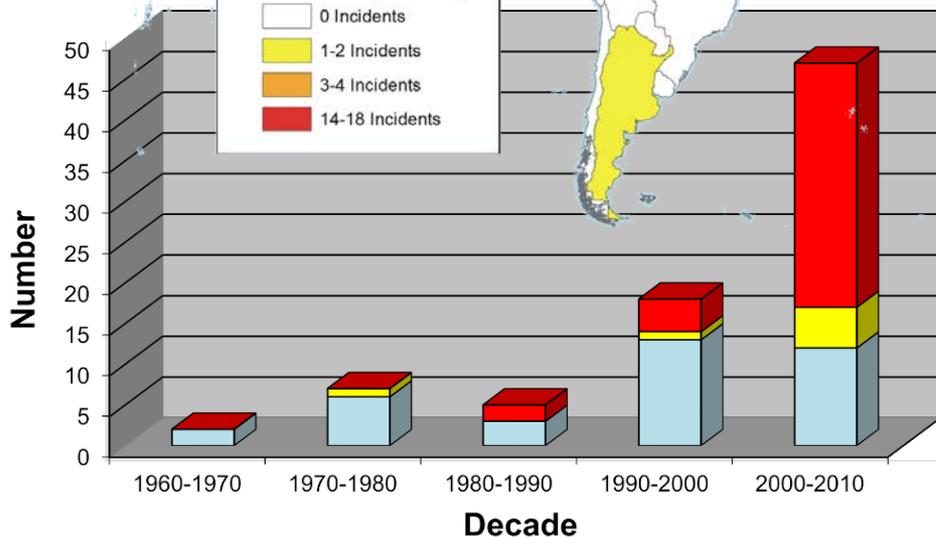
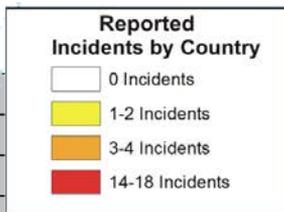
*Robert Johnson, Argonne National Laboratory, [rlj@anl.gov](mailto:rlj@anl.gov)*

# *Talk Overview*

- Review of historical malicious use events involving radioactive material
- General threat environment
- Orphan sources – definitions and background
- Events of concern involving end of life sources

***End of life sources pose security concerns and have been a demonstrated historical security risk.***

# Historical Malicious Use Plots Involving Radioactive Material



# Historical Cases Demonstrate RDD Possibility



## Cs-137 Attack, 1972

Texas petroleum engineer obtained an oil exploration device containing Cs-137 and used it to irradiate his estranged son, causing the child significant bodily harm.



## Cs-137/Ir-192 Attack, 1998

South Korean medical doctor stole Cs-137 and Ir-192 brachytherapy sources and attempted to murder his mistress by hiding them in her car.



## Co-60 Attack, 1993

Unknown perpetrator murdered the manager of a Russian packaging company using a Co-60 industrial source hidden in his chair.



## Ir-192 Attack, 2001

Chinese radiation technologist obtained Ir-192 radiography sources, fashioned a necklace, and attempted to murder a former girlfriend. Several individuals suffered from radiation exposure.



## Co-60 Attack, 1997

Chinese phosphate plant employee stole a Co-60 industrial source and used it to murder his plant manager by hiding it in his office.



## Ir-192 Attack, 2003

Chinese nuclear medicine researcher illegally obtained an Ir-192 radiography source and attempted to murder a colleague by hiding it in his office. 74 people suffered from exposure before it was discovered.



## Cs-137/Am-241 Extortion, 1998

Am-241 and Cs-137 oil exploration sources were stolen at gunpoint while in transit to Colombian job site. The thieves, who included a company employee, threatened to disperse the material if not paid.

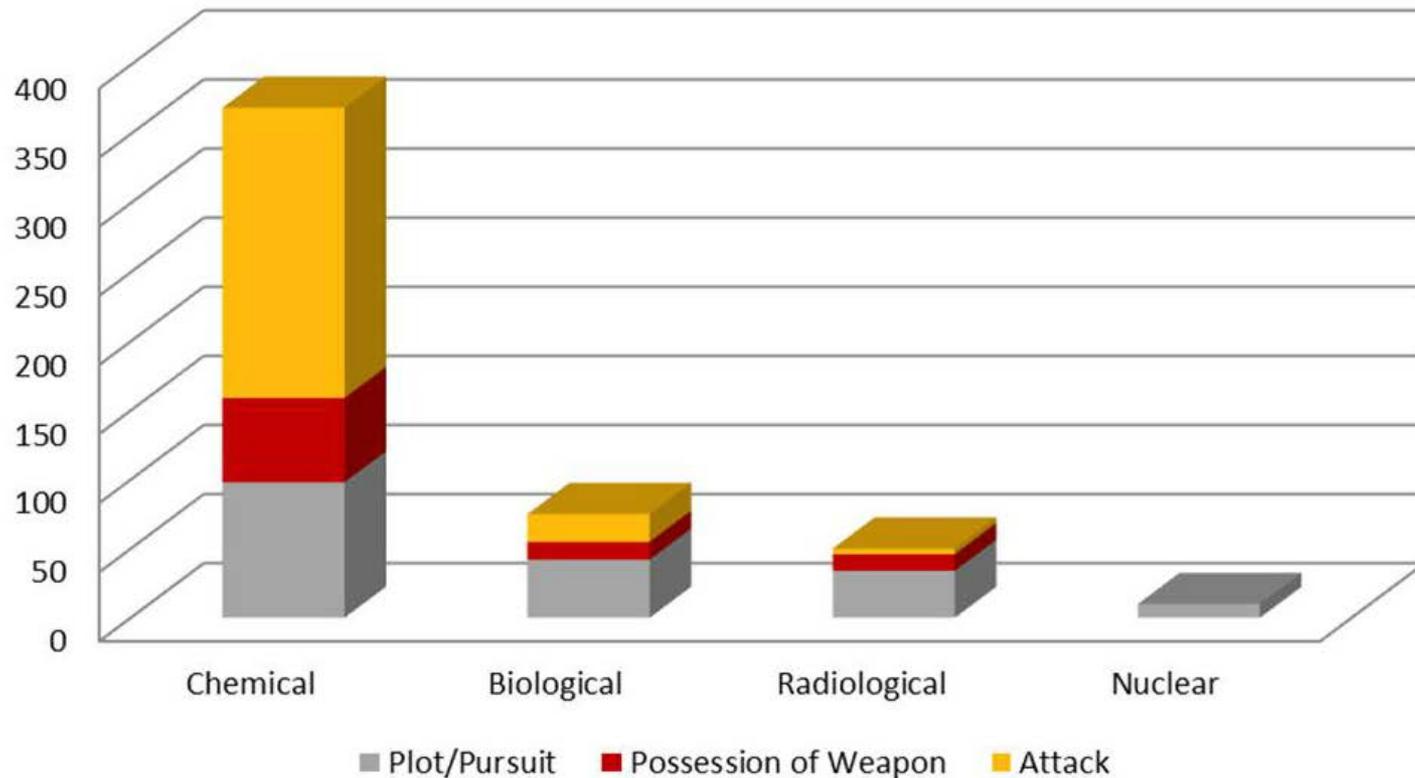


## Cs-137 Attack, 2006

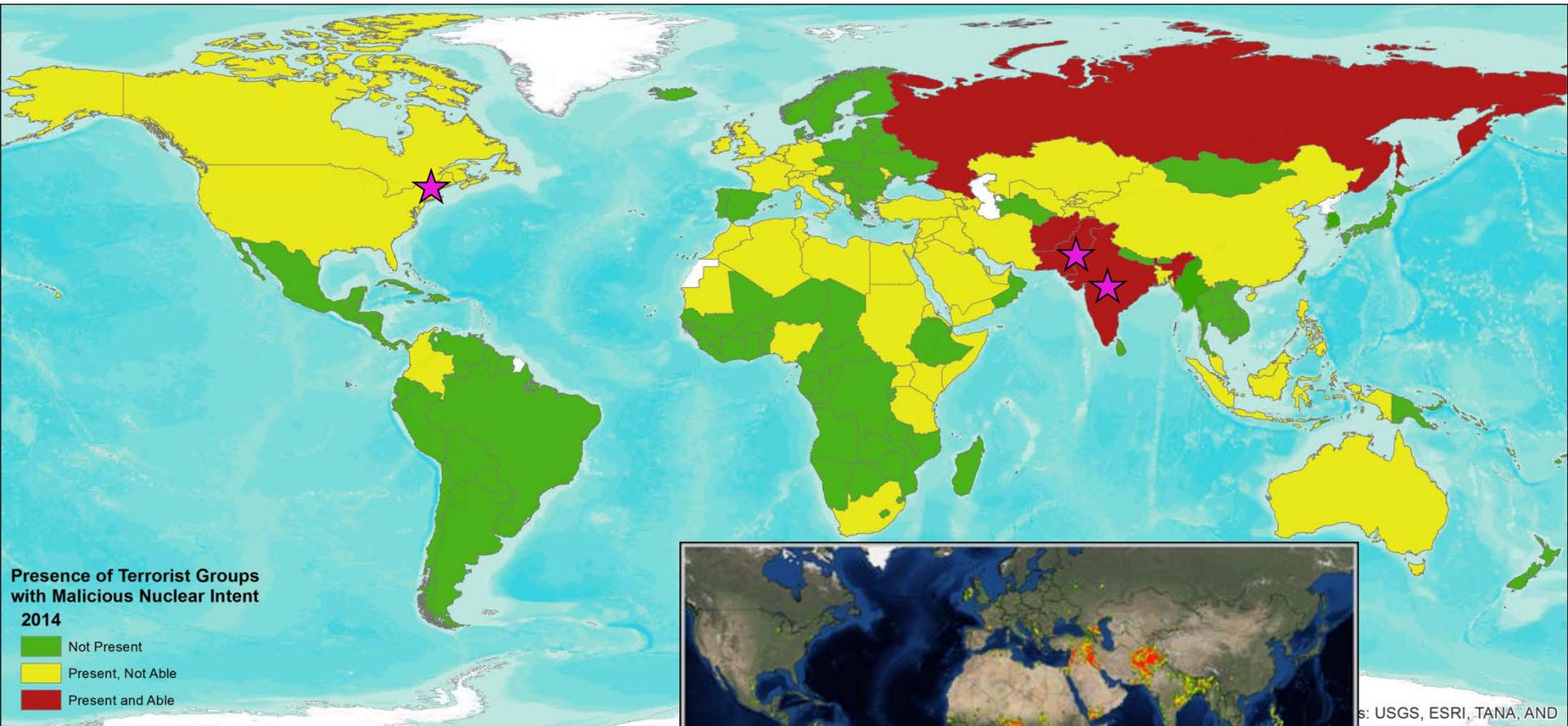
Unknown perpetrator attempted to murder a Chinese university professor by hiding a Cs-137 source in his office.

# ***START CBRN Historical Review***

## CBRN Agent and Event Type



# 2014 NTI Global Nuclear Threat Assessment



# ***What Are Orphan Sources?***

- The IAEA definition: “Radioactive sources that are outside of regulatory control are called "orphan sources" for short. They may never have been subject to regulation, or they may have been regulated initially but then were abandoned, lost, misplaced, stolen, or removed without authorization. Some sources may not be formally "orphaned" but their control may be weak and therefore vulnerable to being mishandled or lost.”

# What Kinds of Sources are Orphaned?



Soil Moisture/Density  
Gauges - 1.4 GBq Am-  
241 & 0.3 GBq Cs-137



Oil and Gas  
Exploration Logging  
Devices – Cs-137 &  
Am-241 GBq range



Industrial Gauges  
(Am-241, Co-60,  
Cs-137) - MBq to  
GBq range



Radiography  
Cameras (Ir-192,  
Se-75, Co-60) -  
GBq to TBq range

# What Kinds of Sources are Orphaned?



Self-Shielded Irradiators  
(Cs-137 & Co-60) - TBq  
range



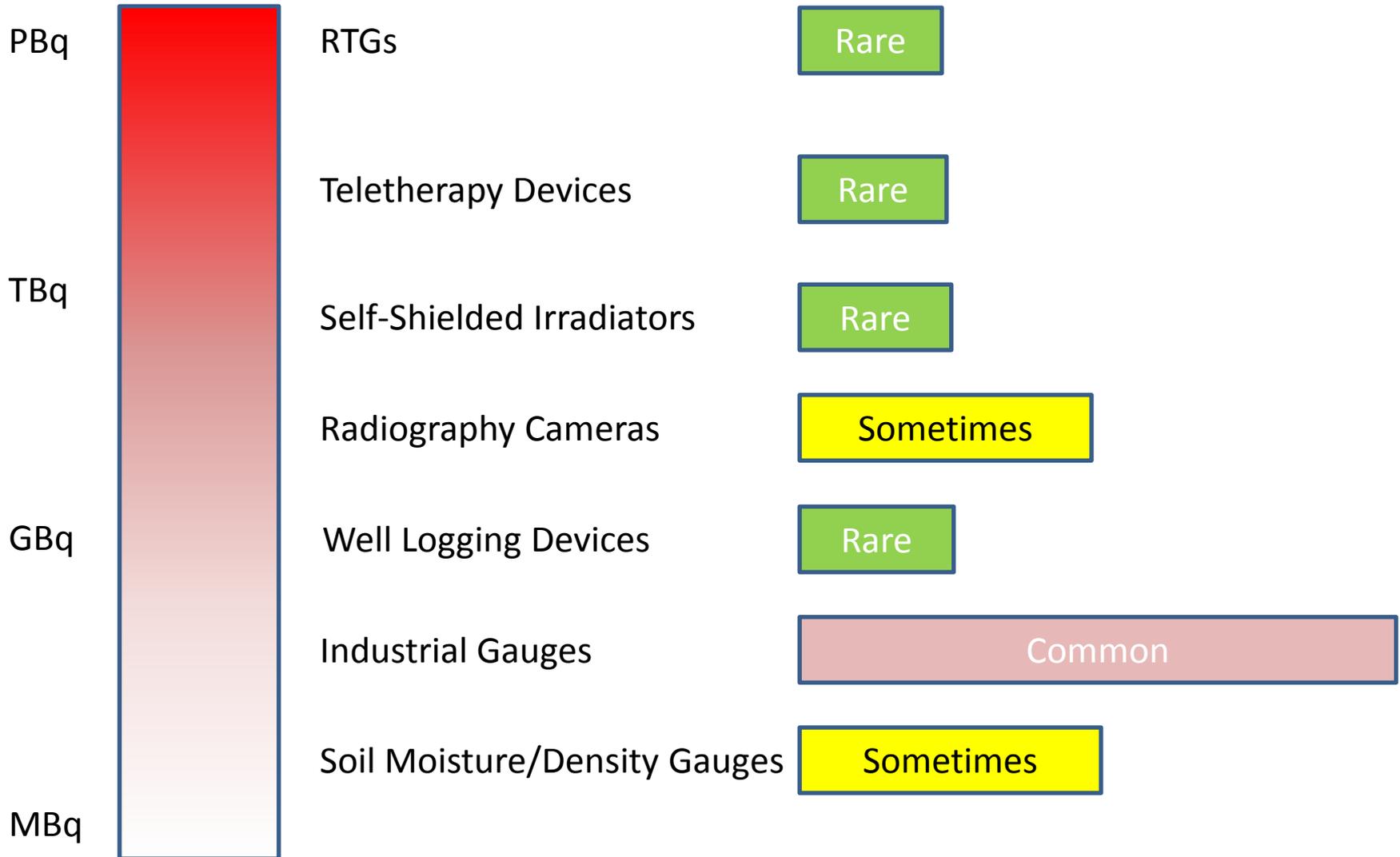
Teletherapy (Co-60) -  
TBq range



Radioisotope  
Thermoelectric  
Generators (Sr-90) –  
PBq range



# *With What Frequency?*



# *What Harm Can Be Done with These Sources?*

- 2004, Dhiren Barot arrested in U.K. on terror charges
- Plot involved purchase of 10,000 smoke detectors for use in “smoky bomb”
- Inspired by 1999 France accident involving cargo fire and 900 smoke detectors
- 2014 subsurface WIPP accident released Am-241 to the air, shutting down facility and resulting in measurable quantities of airborne Am-241 25 miles away
- Typical Am-241 exploration device contains more than 1,000 times the activity of Barot’s plot

- 2003, a Chinese nuclear medicine researcher named Gu Jiming illegally obtained an Ir-92 radiography device
- Placed source material above ceiling tiles in colleague’s office
- Exposure took place for more than 2 months before discovery
- 74 individuals were exposed in all, several with very serious medical complications as a result
- Regular international shipments of fresh Ir-192 can exceed the amount used by Gu by one or two orders of magnitude

# ***How Are Sources Orphaned?***

- Bankruptcy/facility closure
- Neglect
- Theft and abandonment
- Transportation loss
- Illicit disposal

# Bankruptcy/Facility Closure Cases



- U.S. Gamma Knife facility closed in 2008 (100 TBq Co-60)
- Security systems shut down – only



- Scrap cargo in Italy contained significant Co-60 source in 2010
- Shipment originated in Saudi



- Abandoned foundry in Eastern Europe
- Five to seven Co-60 devices stolen from



- Abandoned steel mill in Africa
- More than 200 devices with radioactive material, mostly but not all Cs-137
- Significant concerns about security – still an issue in 2013

# Neglect



- U.S., 2009
- Fabric company building demolished
- 12 Am-241 gauges (7 reportedly missing) found during demolition
- Since 2002 22 cases of Am-241 losses in U.S.



- India, 2010
- End of life Co-60 research irradiator improperly sold for scrap by University (unused since 1985)
- Multiple source pieces located in Delhi scrap yards
- At least eight people hospitalized and one fatality



- Mexico, 2013
- End of life Co-60 teletherapy device stolen during shipment
- Minimal security present during shipment
- Eventually recovered, but only after exposure had taken place

# *Theft & Abandonment*

- Mexico, 2014
- Truck carrying Ir-192 radiography camera stolen
- Device found one day later abandoned a few miles from where truck was stolen



- Nepal, 2014
- Spent Ir-192 brachytherapy sources “lost” en-route to Kathmandu by vehicle
- Package found abandoned by a tea shop owner one day later



- U.S., 2014
- Remains of a package containing DU shield and Mo-99 generators found in NYC vacant lot
- Had been shipped 6 months prior and never arrived at destination



Mo-99/Tc-99m  
Generators

# *Illicit Disposal Cases*

- U.S., 2012
- 80 yr old 40 GBq Ra-226 medical source recovered in scrap load
- Despite advertisement and fears of public exposure, no one stepped forward to claim



- U.S., 2013
- Cs-137 industrial gauge discovered in U.S. paper shipment refused by China
- Device detected by port monitor upon shipment return



- Lithuania, Various Years
- Pu-239 smoke detectors found discarded in various locations



# ***Peculiarities of End of Life/ Orphan Source Vulnerabilities & Threats***

- Orphan sources, by definition, have no one purposefully providing security
- The acquisition of an orphan source for malicious purposes by a perpetrator would be unnoticed and unreported
- Storage settings for end of life sources often do not have the same level of security controls as would be found for a device in active use

# *Once Loose, Sources Are Difficult to Recover*

Unless in relatively close proximity to a missing device, devices can be hard to detect



**Austin, Texas, July 2011.** Theft of 1.2 TBq (34 curie) Ir-192 radiography camera from parked truck with surveillance video but no truck alarm. Despite intensive searches by ground and air and offer of reward, never recovered.

**Pecos, Texas, September 2012.** Loss of 555 GBq (15 curie) Am-241/Be device between Pecos and Odessa, Texas. Presumably fell off truck. Despite intensive ground and air searches, device remained unrecovered for several weeks until found by member of public lying in middle of dirt road.



# *Take Away Points*

- Historical and on-going evidence of terror group interest in radioactive material
- End of life and orphaned sources present their own unique vulnerabilities
- Once on the loose, an orphan source can be very difficult to recover

***Goal has to be preventing loss.***