HARVARD Kennedy School
BELFER CENTER
FOR SCIENCE AND INTERNATIONAL AFFAIRS

The danger of nuclear terrorism and what can be done about it

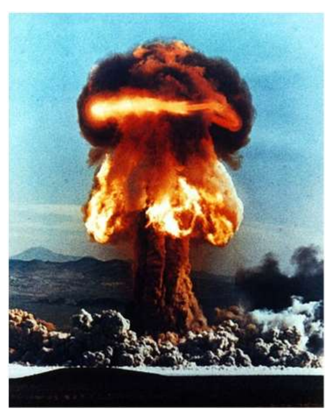
Matthew Bunn
Professor of Practice, Harvard Kennedy School
MIT, "Social Problems of Nuclear Power"
22 October 2020
belfercenter.org/managingtheatom
scholar.harvard.edu/matthew_bunn

1

3 types of nuclear terrorism

2

- Nuclear explosives
  - Incredibly catastrophic
  - Difficult for terrorists to accomplish (though not as implausible as some believe)
- Nuclear sabotage
  - Very catastrophic *if* highly successful (limited if not)
  - Could cause a Fukushima-scale accident, or worse
  - Also difficult to accomplish
- "Dirty Bomb"
  - "Weapons of mass disruption" – few if any deaths, but potentially $10s of billions in disruption, cleanup costs
  - Far easier to accomplish

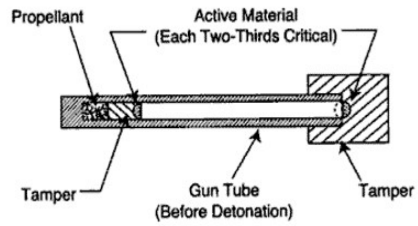

Source: DOE

2

With nuclear material, terrorists may be able to make crude nuclear bombs

3

- With HEU, gun-type bomb – as obliterated Hiroshima – very plausibly within capabilities of sophisticated terrorist group
- Implosion bomb (required for plutonium) more difficult, still conceivable (especially if they got help)
  - Doesn't need to be as complex as Nagasaki bomb



Source: NATO

Doesn't take a Manhattan Project -- >90% of the effort was focused on producing nuclear material. And making a crude terrorist bomb is *far* easier than making a safe, reliable weapon

3

Terrorist groups have pursued all three

4

- Aum Shrinkyo – Japanese terror cult
  - Conducted nerve gas attacks in Matsumoto in 1994 and in Tokyo subways in 1995
  - Previously had focused efforts to get nuclear, biological weapons
- "Core" al Qaeda
  - Focused effort to get nuclear weapons
    - Reported directly to Zawahiri
    - Carried out conventional explosive tests for the bomb program in desert
  - Also considered attacks on nuclear reactors
  - Affiliates pursued rad material for "dirty bomb"
- Chechen terrorists
  - Planted dangerous radiological source in a Moscow park as warning – threatened to use "dirty bombs"
  - Repeatedly threatened, planned attacks on reactors
  - Russian officials report catching terrorist teams scoping nuclear weapon storage sites, transports

4

The Islamic State – good news and bad news

5

- Ideology envisions final war with "crusader" forces – powerful weapons needed
- Islamic State produced, used its own chemical weapons
- Clear capacity for disciplined manufacture, technical innovation
  - Manufactured mortars, shells, other arms to precise tolerances
  - Drone and IED efforts repeatedly built, tested new ideas
- Monitoring of Belgian nuclear official hints at nuclear interest
  - Hours of monitoring of official's private home, by operatives involved in Paris attacks
  - Senior official at facility with HEU, rad sources, research reactor…
- BUT: IS did nothing with the large Co-60 sources under their control
  - Large sources were in territory they controlled, now back in government hands

5

Rapidly evolving threats

6

- ISIS and future groups
  - Not mentioned in 1/14 threat assessment
  - Seized much of Iraq and Syria by 6/14
  - How will these groups evolve next?
- Cyber
  - Constant discovery of new vulnerabilities
  - Nuclear facility requirements still at early stages in many countries
- Drones
  - Commercially available drones getting more advanced every year
  - Could nable wide range of tactics that require defenders to rethink approaches
- What's next?
  - How to keep up with the threat while having some regulatory stability?

6

A recent example: insider sabotage and a cleared terrorist at Doel-4 nuclear plant

7

- August 2014: An insider at Doel-4 reactor in Belgium drains lubricant, destroys reactor turbine
  - ~$200 million damage
  - Investigators unable to find culprit
  - Sabotage intended to cause economic damage, not radiation release
- Investigation finds that long before, contractor Ilyass Boughalab had access to vital area
  - Passed security clearance review in 2009
  - In late 2012, left to fight for terrorists in Syria (reportedly killed later)
  - Later convicted as part of "Sharia4Belgium" terrorist group

Source: Kristof Pieters

7

"Dirty bombs" – a serious ongoing threat

8

"My reporting leads me to conclude that the most ominous terrorist threat—based on the relative ease of pulling off such an attack, the possible damage it could do, and, most of all, the danger of overreaction to it—is the dirty bomb."

— Steven Brill, *The Atlantic,* September 2016

8

An intelligent adversary fundamentally changes probability estimates

9

- Probability is a method developed for random events – planned human actions are not random
- Earthquakes will not:
  - Preferentially strike the site least able to protect against them
  - Observe the defenses and attempt to bring enough capability to defeat them
  - Consciously plan to cause both primary and backup systems to fail
- Terrorists will seek to do all of those things
  - In security, failures *are not independent*
  - In security, the past is a less reliable guide to the future – adversaries learn and evolve
- Nevertheless, estimating the chance of different events – in concert with other methods – can help structure thinking, identify weak points to be addressed

9

Nuclear material is not hard to smuggle – plutonium box for first-ever bomb

10

Source: Los Alamos

10

Assessing the nuclear terrorism risk

11

- A simple model of the risk can help clarify thinking (though it cannot provide "the answer")
  - *N* terrorist groups seeking nuclear weapons
  - P_a annual chance that a group will make a nuclear acquisition attempt – rather than investing those resources in non-nuclear terror
  - Group may choose (each with some probability) to try to:
    - Buy material on the nuclear black market
    - Instigate an insider theft
    - Instigate or carry out an outsider theft
    - Get material from a state
  - Each has some probability (P_s) of success
  - Once it has material, the group then has some probability (P_w) of being able to turn the material into a workable bomb
  - The group then has some probability(P_d) of deciding to, and being able to, deliver and detonate its bomb

11

Two examples: optimistic and pessimistic assessments

12

	Example 1	Example 2
No. of plausible terrorist groups	2	1
Chance of acquisition attempt per year	0.3	0.1
Black-market: chance to be chosen, then to succeed	0.5, 0.2	0.5, 0.1
Insider theft: chance to be chosen, then to succeed	0.3, 0.2	0.3, 0.1
Outsider theft: chance to be chosen, then to succeed	0.15, 0.15	0.15, 0.1
From state: chance to be chosen, then to succeed	0.05, 0.1	0.05, 0.05
Chance of making a workable bomb	0.4	0.2
Chance of delivering and detonating bomb	0.7	0.4
Result: 10-year probability of nuclear terrorism	0.27	0.0078

Even 0.75% chance over 10 years is far too high a risk of a city being devastated by a terrorist nuclear bomb

12

Assessing the risk of theft at particular nuclear facilities and transports

13

- Risk of theft at a particular facility or transport:
  - Probability of theft attempt (unknown, presumably reduced by stronger security measures)
  - Probability theft attempt would succeed, determined by
    - Probability distribution of adversary capabilities
    - Capabilities security system can protect against
  - Consequences: probability stolen material could be used to make a bomb, determined by:
    - Adversary capabilities
    - Material quantity
    - Material quality
- Thieves will seek to observe, exploit security weaknesses

13

Assessing the risk of sabotage at particular nuclear facilities

14

- Risk of a sabotage attempt at a particular facility or transport:
  - Probability of sabotage attempt (unknown, presumably reduced by stronger security measures)
  - Probability sabotage attempt would succeed, determined by
    - Probability distribution of adversary capabilities
    - Capabilities security system can protect against
    - Difficulty of catastrophic sabotage (related to safety measures)
  - Consequences, determined by:
    - Quantity of radioactivity present
    - Potential to mobilize, disperse the material
    - Nearby populations, economic and other assets
- Saboteurs will seek to observe, exploit security weaknesses

14

Comparing nuclear safety and nuclear security risks: the historical record

15

- U.S. safety goal: 1/10,000 per reactor-year chance of major core damage; 1/100,000 chance of major release
  - Obviously haven't met this goal so far
  - 4 reactors with major releases (Chernobyl and 3 at Fukushima Daichi) in 16,000 reactor-years of operation – 1/4,000 reactor-years
  - Other core damage events (TMI, Fermi I…)
  - But goal remains valid – and given horrifying consequences, goal for preventing nuclear terrorist attack should be *more* stringent
- Nuclear theft:
  - ~300 global facilities with HEU or Pu -- ~ 7,500 facility-years over last 25 years
  - ~20 seizures of stolen HEU or Pu in that time (some from same theft)
  - > 1/400 per facility-year
  - Most from Russia (but also most facilities there); several seizures may be from same theft – but still, shows rate far too high

15

Comparing nuclear safety and nuclear security risks: the historical record (II)

16

- Nuclear sabotage
  - During ~16,000 reactor-years of operation:
  - 1 case in which insider placed explosives on steel pressure vessel and detonated them*
  - 1 case (very recent) in which insider sabotage destroyed reactor turbine
  - 1 case in which terrorists overwhelmed and captured the guard force, were in full control for extended period before leaving when off-site response arrived*
  - 1 case of RPG being fired at, hitting reactor
  - Multiple cases of terrorist groups planning attacks on reactors
  - ~ 1 major incident per 3-4,000 reactor-years

Both theft and sabotage risks appear to be very high compared to safety goals

*reactor not yet operational

16

Key steps to reduce the nuclear terrorism risk

17

- Police and intelligence:
  - Detect and disrupt terrorist nuclear-related plots
  - Aum Shinrikyo disrupted after nerve gas attacks
  - Multiple al Qaeda-related plots successfully disrupted after 9/11
- Security for weapons, materials, and facilities:
  - Make it harder for terrorists to get essential ingredients of weapon or sabotage a facility – major progress in last quarter century
- Block nuclear smuggling
  - Radiation detection, targeted police and intelligence
  - Enormous challenge: once stolen, material could be anywhere
- Prepare to reduce consequences

Effective security for nuclear weapons, materials, facilities as the highest leverage in reducing the risk

17

North Korea and Iran are likely small parts of the nuclear terrorism problem

18

- Nuclear security:
  - North Korea has only a few bombs' worth of plutonium in a tightly controlled garrison state – theft very unlikely
  - Iran has not begun to produce weapons-usable material – has only a small amount of HEU research reactor fuel
- Conscious state transfer:
  - Regimes bent on maintaining power unlikely to take the immense risk of providing nuclear bomb material to terrorist groups who might use it in a way that would provoke overwhelming retaliation
  - Transfers to other *states* – who are likely to be deterred from using nuclear weapons – a very different act
- High-level "rogues" within states
  - As stocks of material grow, could an "A.Q. Kim" sell secretly?
- State collapse:
  - Could have worrisome "loose nukes" scenario

18

Spread of nuclear power <u>need not</u> increase terrorist nuclear bomb risks

19

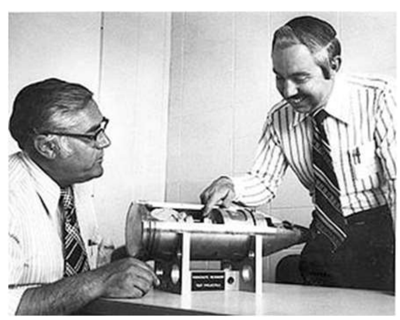
- Most nuclear reactors do not use nuclear material that can readily be used in nuclear bombs:
  - Low-enriched uranium fuel cannot be used to make a nuclear bomb without technologically demanding further enrichment
  - Plutonium in spent fuel is 1% by weight in massive, intensely radioactive fuel assemblies (but R-Pu <u>is</u> weapons-usable)
- Reprocessing (separating plutonium from spent fuel) could increase risks, requires intensive security and accounting
  - Poor economics, few additional countries pursuing – South Korea and China only countries currently considering shift to reprocessing
  - Reprocessing does not solve the nuclear waste problem – still need a nuclear waste repository
- Power reactors <u>do</u> pose potential targets for sabotage
  - Sabotage would mainly affect nearby countries, global nuclear industry – strong security measures can reduce the risk

19

Nuclear security: the global picture

20

- Global stockpiles include:
  - ~13,000 nuclear weapons
  - ~ 520 tons of separated plutonium
  - ~1335 tons of HEU (+/- 125 tons)
  - <1/3 of plutonium and HEU is physically in nuclear weapons
- Stocks located in 100s of buildings, bunkers, in ~ 22 countries
- Widely varying security
- No global rules specify how secure nuclear weapons or the materials to make them should be



W-48 nuclear artillery shell, one of many thousands of tactical nuclear weapons that have been dismantled

Source: U.S. Department of Energy

Theft of 0.01% of world stockpile could cause a global catastrophe

20

Global nuclear security: A system no one designed…

21

- Imagine a system with100s of nodes:
  - Little or no central control
  - Failure of any node could cause catastrophic damage
- To reduce risk in such a system, you could try to:
  - Strengthen each node (e.g., technical cooperation)
  - Increase central control (e.g., international accords)
  - Reduce the number of nodes (e.g., nuclear material removals)
  - Reduce the consequences of node failure (e.g., reactors where failure could cause only limited release, materials difficult to use in a bomb)
  - Increase ability to recover after a node failure

No engineer in his or her right mind would design such a system

21

Nuclear security is quite different from nuclear safety, in several dimensions

22

- Safety: preventing, preparing for *accidental* events
- Security: preventing, preparing for, *intentional* human actions
  - Changes the statistics – multiple failures no longer independent
- Many overlaps – some conflicts
- Nuclear security involves:
  - Lower, more controversial threat perception (no widely known incidents)
  - Lower public interest
  - More secrecy
  - Less organizational focus, resources
  - More separation from the rest of the operating organization

Source: The Millenium Report

22

Insider threats are the most dangerous nuclear security problem

23

- The known HEU and Pu thefts, and most sabotages, involved insiders
- People don't want to believe their friends and colleagues could betray the organization
  - Leads to serious lapses in protection against insider threats
- Getting people to report suspicious behavior is *very* difficult
- Often even obvious "red flags" go unreported, unaddressed
- Bunn-Sagan book offers case studies, "Worst Practices Guide" on lessons learned from past mistakes

http://www.belfercenter.org/publication/insider-threats

23

The international nuclear security framework

24

- Key purpose of *international* and *national* frameworks is to ensure effective *local* nuclear security
  - International accords seek to influence national policies, which seek to influence local action – very indirect effect
- International framework includes many elements – a "regime complex," not a single regime
  - Binding agreements
  - International recommendations
  - Technical cooperation
  - Summits and other high-level discussions
  - IAEA services
  - Requirements of supply agreements
  - Best practice exchanges
- Constrained by complacency, sovereignty, secrecy, politics, bureaucracy, cost…

24

Substantial nuclear security progress over past 25 years…

25

- Most egregious weaknesses essentially all resolved
- U.S. in particular has spent billions helping others improve – and launched series of "nuclear security summits"
- > 50% of all countries that once had weapons-usable material on their soil have eliminated it
- Many particular improvements
  - Most countries that had no armed guards (even for plutonium and HEU) have corrected that
  - Most countries with major nuclear activities now have a "design basis threat" operators must protect against
  - More countries doing realistic assessment, testing, of nuclear security systems
  - More attention to insider threats
  - More attention to security culture

25

With "nuclear security summits" in the past, progress is slowing…

26

- Little high-level political attention, little sense of urgency
- U.S. international nuclear security programs dramatically reduced
- Some key elements of cooperation cut off or slowed
  - Almost no remaining US-Russian cooperation, post-Crimea seizure
  - Very modest cooperation with wealthy countries (some of which have a <u>lot</u> of material)
  - U.S.-China, U.S.-India cooperation real but modest
  - U.S.-Pakistan cooperation was substantial, most urgent agreed items completed – many items Pakistan not interested in cooperating on
  - Most politically, technically feasible removals of nuclear material already done
- Still much to do – but each step forward now more difficult

26

Further reading and background material

27

- *Revitalizing Nuclear Security in an Era of Uncertainty* (2019): https://www.belfercenter.org/NuclearSecurity2019
- *The U.S.-Russian Joint Threat Assessment of Nuclear Terrorism*: https://www.belfercenter.org/publication/us-russia-joint-threat-assessment-nuclear-terrorism
- *Insider Threats* (Cornell, 2018)
- Selected presentations and publications: https://scholar.harvard.edu/matthew_bunn/nuclear-terrorism-and-nuclear-security?admin_panel=1
- Full text of Managing the Atom publications: *http://belfercenter.org/mta*

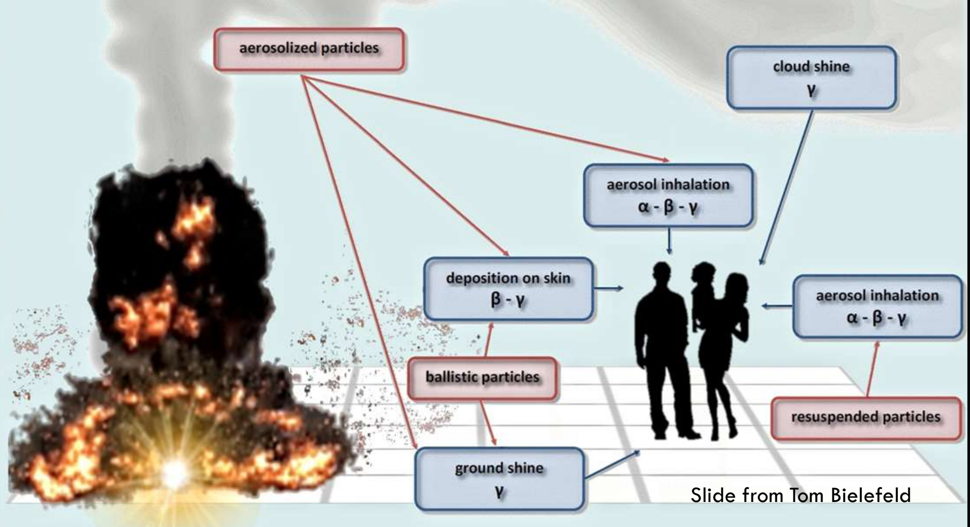
27

For additional information…

28

28

Scenario: Dirty Bomb From High-Activity Medical or Industrial Radioactive Source



Slide from Tom Bielefeld

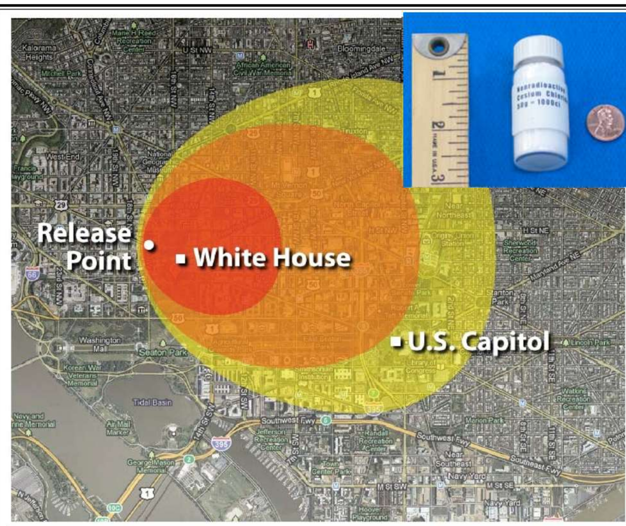
29

Cs-137 "dirty bomb"

30

- Some form of dangerous sources used in hospitals, industry, in almost every country -- often weak security
- Cs-137 is esp. dangerous – powder easy to disperse, very hard to clean

Source: Congressional Research Service, modeling by Sandia National Laboratories, 2010



Effects and Actions

	Area km²	mi	Equivalent Dose (rem)	Exceeds relocation PAG for which year:	Population	All Cancers	Fatal Cancers
(red)	2.10	0.81	>2.00	First year only	38,000	233	159
(orange)	7.60	2.93	>0.500	Any subsequent year	94,700	278	189
(yellow)	13.2	5.10	>5.00	50 years (cumulative)	125,000	461	314

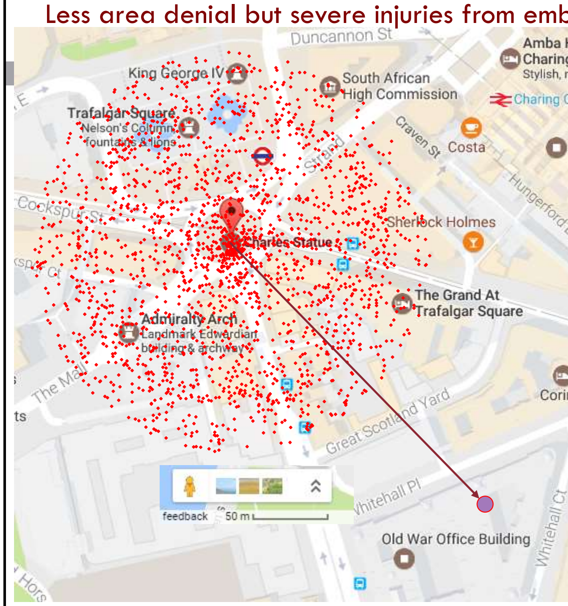
Areas and counts are cumulative. RDD detonated at 38.9 N, 77.0 W. PAG: Protective Action Guide

30

Analysis

Scenario: Co-60 Teletherapy Source

Less area denial but severe injuries from embedded Co-60 pellets.



- Pellets Scatter as ballistic projectiles
- ~ 100 m radius
- Embedded pellets, a prompt injury hazard
- Entire ~100 m radius zone is rad-hot (> 10 mSv/hr)
- Adversaries *could* also find ways to aerosolize metal sources

Slide from Len Connell

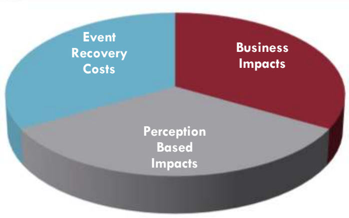
31

31

Analysis

Area Denial RDD: Economic Impacts

Three components.



Social costs, hard to quantify:
- Increased fear/anxiety
- Historic buildings quarantined
- Forced relocation from homes
- Increased security/loss of freedom

- ***Event Recovery Costs*** – 1 yr (typically assumed)
  - Survey, Decontamination/Demolition, Disposal, New Construction, Relocation, Compensation, Health Care
  - Reality-It could take much longer than 1 yr.
- ***Business Impacts*** – < 1 yr (typ.)
  - Direct – Lost GDP from business affected inside denied area
  - Indirect – Lost GDP from business affected outside denied area
  - Induced – Lost GDP from reduced spending by affected households
- ***Perception Based Impacts*** – can persist, many years
  - Willingness to purchase goods/services from region
  - Willingness to invest in region
  - Willingness to work in the region

For a nationally significant RDD, these costs can each approach $10's of Billions

Slide from Len Connell

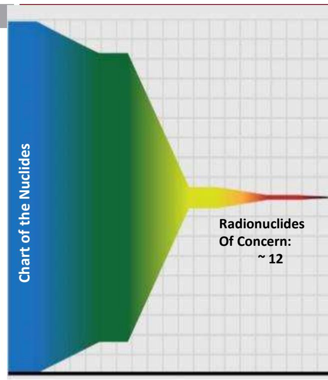
32

32

Analysis

Radionuclide Properties

The Power to Contaminate (PTC) measures area denial potential.



Nuclide	$T_{1/2}$	Dose Rate at 1 meter (mSv/hr per Ci)	Typical Form	Area Denial PTC* (Ci/km²)	Typical Use and Activity
Co-60 (β,γ)	5.3 yr	14	Hard Metal	10	Irradiators & Teletherapy (~10,000 Ci)
Cs-137 (β,γ)	30 yr	3.8	Salt Powder	40	Irradiators (~1000 Ci)
Ir-192 (β,γ)	74 d	6.0	Hard Metal	100	Portable Radiography (~100 Ci)
Am-241/ Be (α,γ, n)	433 yr	0.05	Oxide Powder	~ 10	Portable Well Logging (~ 10 Ci)

Perfect Terrorist

***Power to Contaminate** (**PTC**) = Radionuclide ground contamination level in Curies, uniformly spread over 1 sq. km, that would trigger the US EPA Relocation Protective Action Guide (PAG) of 20 mSv/yr in the first year after the incident. Approximate values. Based on reducing risk of delayed cancers.

PTC values are similar to IAEA Category 2 thresholds

Slide from Len Connell

33

33

Security for radiological sources – a global cooperative effort

34

- NNSA works to protect, replace dangerous rad soures worldwide
- IAEA offers recommendations, reviews, training, limited assistance – all voluntary
  - IAEA has no authority to regulate nuclear or radiological security
- Nuclear security summits raised issue to highest political levels – but how to maintain that momentum?
- U.S. leadership on radiological security includes "walking the talk"

Recovery of stolen radioactive source in Mexico. Source: NNSA

34

Steps to reduce the nuclear theft and sabotage risks

35

- Nuclear theft:
  - Reduce the number of facilities and transports with HEU and Pu (fewer facility-years per year)
    - More sites, transports with separated plutonium means more risk
  - Increase security for remaining facilities (lower chance of theft per facility-year)
    - Better protection against both outsiders and insiders
    - Critical issue: strengthening security culture – "Good security is 20% equipment and 80% culture."
- Nuclear sabotage:
  - Increase security for reactors, other high-consequence facilities
  - Increase passive safety (making large-scale release more difficult for saboteurs to achieve)
    - Example: move cooled spent fuel to dry casks

35

Public fear of radiation increases disruption from a terrorist radiation incident

36

- The very word "radioactive" provokes fear
- Public doesn't understand that radiation is all around us – and has deep distrust from past incidents, coverups
- After an incident, radiation will be detectable in far larger areas than where it's a hazard
- Scariest items in the media will get the most views, pickup
- Who will have the public credibility to say what's safe, and be believed?
  - Major unsolved public education problem

Source: Air Photo Service, Japan

36

First responders can enter contaminated areas without endangering their lives

37

- Typical maximum permitted dose to emergency workers is 5 rem (0.05 Sievert or 50 mSv)
  - EPA guidelines permit higher doses if needed to save critical infrastructure, large populations
  - 5 rem would increase lifetime risk of dying of cancer by ~ 0.3%
  - “normal” lifetime risk is ~20%
- Takes ~100 rem (1 Sv) to make you feel sick
  - 20 times maximum
- ~500 rem (5 Sv) is fatal for about half those who receive this dose
  - 100 times maximum
- NNSA can help with equipment (e.g., detectors, masks), procedures, training to limit risk to 1st responders

Going into the contaminated area is <u>not</u> a suicide mission

37

Better security for radiological sources can reduce the risk at low cost

38

- In-device delay – design devices to rad source can’t be removed without special tools
- Alarms, security cameras – linked to local police
- Security surveys can help identify low-cost, sustainable improvements
- Transport security is a particular issue – multiple incidents of theft from vehicles, or of vehicles themselves
- Training, exercises needed to for 1st responders to prepare to respond

Source: GAO

38

Replacing radiological sources with other technologies – permanent risk reduction

39

- For many uses, radiological sources can be replaced with other technologies that emit no radiation once turned off
  - Nothing for terrorists to steal or sabotage
- National Academy of Sciences panel called for replacement of Cs-137 sources in particular
- France has already replaced its Cs-137 blood irradiators
- So has Norway
- Japan has replaced >70% of its Cs-137 irradiators

Source: CRS

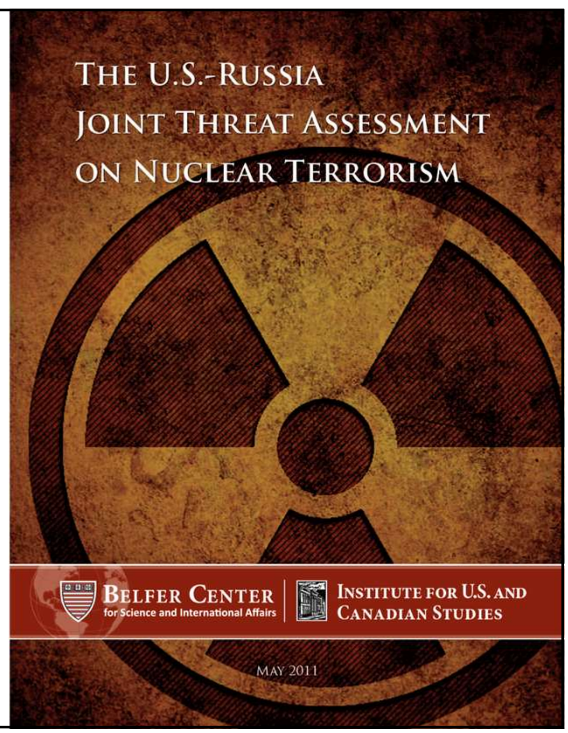
39

A joint U.S.-Russian view

- First ever U.S.-Russian joint threat assessment
- Concludes the danger is real, urgent action is needed to reduce it
- Endorsed by broad range of retired military, intelligence experts

http://belfercenter.ksg.harvard.edu/publication/21087/

40



40

Key core al Qaeda nuclear operatives still at large

41

Ayman al Zawahiri  Source: FBI	Now head of the group. Nuclear project reported directly to him.
Abdul Aziz al-Masri  Source: NCTC *aka* Ali Sayyid Muhamed Mustafa al-Bakri	CEO of al Qaeda's nuclear program, oversaw explosives experiments in Afghanistan.

Sayf al-Adel  Source: FBI	Senior al Qaeda operational planner, reportedly personally approved attempted purchase of 3 nuclear bombs in 2003
"Pakistani Nuclear Expert" 	2003 communications from al Qaeda leaders reportedly approved purchase of nuclear devices if the Pakistani expert confirms they are real – U.S. Government has never identified or found this expert

41

North Caucasus terrorists have pursued nuclear and radiological terrorism

42

- Multiple cases:
  - 2 cases of teams carrying out reconnaissance at nuclear weapon storage sites – 2 more on nuclear weapon transport trains
  - Repeated threats to attack nuclear reactors – terrorists who seized Moscow theater in 2002 considered seizing reactor at the Kurchatov Institute
  - Repeated threats to use radiological "dirty bombs" – buried Cs-137 source in Moscow park
  - Captured documents indicate plan to seize a Russian nuclear submarine (possibly with nuclear weapons on board)

Source: Public Broadcasting Service

42

Adversaries can arise unexpectedly in Japan: the Aum Shinrikyo case

43

- Aum's nuclear efforts
  - Cult leader Shoko Asahara was obsessed with nuclear weapons
  - Repeated shopping trips to former Soviet Union – acquired wide range of conventional weapons, recruited thousands of followers, sought to buy nuclear weapons and materials
  - Purchased farm in Australia, stole enrichment documents – idea to mine, enrich its own uranium
  - Turned to chemical and biological weapons when nuclear proved too slow
  - No intelligence agency was aware of their nuclear, biological, or chemical work until *after* the nerve gas attacks
- Lesson: Watch for unexpected adversaries, even in "safe" countries

Source: Associated Press

43

Attack at Pelindaba, Nov. 8, 2007

44

- Site with 100s of kilograms of highly enriched uranium (HEU)
- Attack by 2 teams of armed, well-trained men, from opposite sides – evidence of insider help
- One team:
  - Penetrated 10,000-volt security fence
  - Disabled intrusion detectors
  - Went to emergency control center, shot a worker there, who raised first alarm
  - Spent 45 minutes inside guarded perimeter – never engaged by site security forces
  - Left through same spot in fence – never caught or identified
- South Africa has since undertaken major nuclear security upgrades, established regulatory design basis threat
- Lesson: 2 teams of well-armed, well-trained intruders, with insider help, attacking with no warning, is a credible threat

44

Coping with creative, determined, evolving adversaries

45

- Nuclear security planning must consider the full spectrum of plausible adversary capabilities
- Adversary capabilities and tactics evolve – DBT from 10 years ago may not match today's threat
- Adversaries may think of attack strategies the defenders have not considered, e.g.:
  - Deception (fake uniforms, IDs, paperwork…)
  - Blocking response forces (e.g., mining the road)
  - Tunneling under or flying over defenses (routine in crimes worldwide)
- Solutions:
  - Consider updating, expanding capabilities in Japan's DBT
  - Assign creative team with "hacker" mentality to probe for weak points
  - Carry out realistic tests with unexpected adversary team tactics

45

The scale of the catastrophe

46

- Tens of thousands killed; tens of thousands more burned, injured, irradiated
  - Radioactive fallout would require large-scale evacuation
- Terrorists may claim they had more bombs hidden in cities, threaten to detonate them unless their demands were met
  - Potential for widespread panic, flight from major cities, resulting economic and social chaos
- Huge pressure on leaders of attacked state to take any action necessary to prevent further attacks – and to retaliate
  - Effects on international affairs likely far larger than 9/11

Notions of sovereignty and civil liberties may be radically altered – every state's behavior affects every other

46

Terrorists might be able to get plutonium or HEU

47

- ~20 documented cases of theft and smuggling of plutonium or HEU, some in kilogram quantities
  - Most recent seizures: Georgia 2010, Moldova 2011
  - Even small thefts suggest vulnerabilities that could be exploited for larger thefts
  - Small seizures may be samples of larger stocks
- Major progress in improving nuclear security
  - Dozens of sites with major security upgrades
  - Dozens of sites all material removed
- But many weaknesses remain, in many countries
  - Protection against only modest threats
  - Lack of on-site armed guards
  - Limited insider protection

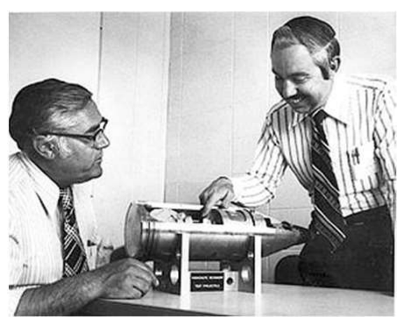
Source: Reuters, from Georgian Interior Ministry

47

Immense global stockpiles of nuclear weapons and weapons-usable materials

48

- ~17,000 assembled nuclear weapons still exist
  - All but ~1,000 in U.S. and Russian stockpiles
- Global stock of separated plutonium is nearly 500 tonnes
- Global stock of HEU is almost 1,400 tonnes (+/- 125 tonnes)
- Nuclear weapons stored at >100 sites
- Weapons-usable nuclear material in hundreds of buildings in dozens of countries around the world



W-48 nuclear artillery shell, one of many thousands of tactical nuclear weapons that have been dismantled

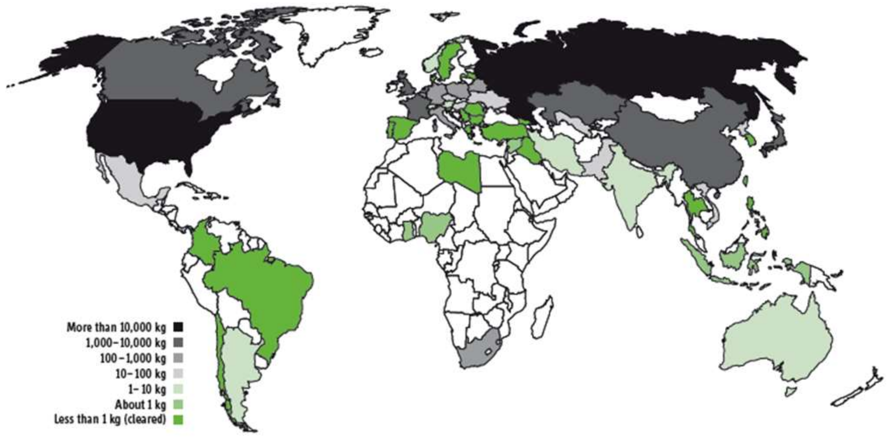
Source: U.S. Department of Energy

Theft of 0.01% of world stockpile could cause a global catastrophe

48

Widely distributed global stockpiles

49



Global Distribution of Civilian HEU Stockpiles

Source: International Panel on Fissile Materials, *Global Fissile Materials Report 2011*

49

What is the evidence that current nuclear security is inadequate?

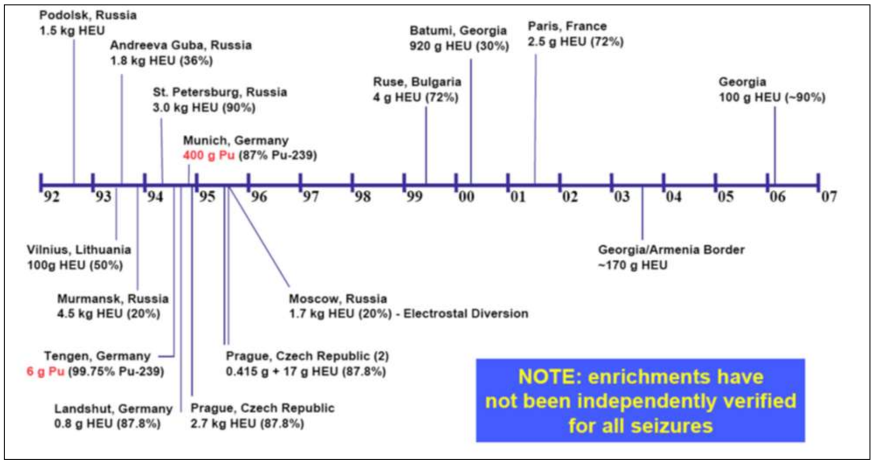
50

- Continuing seizures of weapons-usable material
  - ~20 real cases involving HEU or plutonium since 1992
- "Red team" tests indicate security systems can be defeated by intelligent adversaries looking for weak points
  - Repeated cases in U.S. tests – though U.S. has among the most stringent security requirements in the world
  - Most other countries do not carry out such tests
- Successful thefts and attacks at well-secured non-nuclear facilities – demonstrating adversary capabilities
  - Repeated cases of use of insiders, covert outsider attacks, unusual tactics, succeeding in stealing from/attacking heavily guarded sites (e.g., banks, military bases, diamond centers…)
  - Existing nuclear security measures in many countries demonstrably insufficient to protect against such adversary capabilities

50

Documented seizures, 1992-2006 (more seizures in 2010, 2011)

51



Source: Los Alamos National Laboratory, Tom Bielefeld

51

Recent incidents of concern

52

- U.S., 2012: 82-year-old nun and 2 other protestors penetrate 4 layers of fences (3 alarmed) get right to wall of building holding enough HEU for 1000s of bombs – cameras broken, alarms ignored, major breakdown of security culture
  - Lesson: Can never be complacent about nuclear security, even in countries with strong security rules and large security spending
- Moldova, 2011: Seizure of stolen HEU, from large group, with connection to real buyer – Moldovans report smugglers still at large have at least 1 kilogram HEU
  - Lesson: Smuggling of potential nuclear bomb material an on-going problem – smugglers may be getting more sophisticated
- South Africa, 2007: Attack on HEU site at Pelindaba by 2 armed teams, one team penetrated 10,000-volt security fence, disabled alarms, shot staffer at emergency center
  - Lesson: Nuclear sites must be able to defend against more than one team of sophisticated adversaries, with insider knowledge

52

Security culture matters: Propped-open security door

53

Source: U.S. Government Accountability Office

53

International assessments of the danger of nuclear terrorism

54

"Nuclear terrorism is one of the most serious threats of our time. Even one such attack could inflict mass casualties and create immense suffering and unwanted change in the world forever. This prospect should compel all of us to act to prevent such a catastrophe."

– U.N. Secretary-General Ban-Ki Moon, 13 June 2007

"The gravest threat faced by the world is of an extremist group getting hold of nuclear weapons or materials."

– then-IAEA Director-General Mohammed ElBaradei, 14 September 2009

"We have firm knowledge, which is based on evidence and facts, of steady interest and tasks assigned to terrorists to acquire in any form what is called nuclear weapons, nuclear components."

– Anatoly Safonov, then counter-terrorism representative of the Russian president, former head of the FSB, 27 September 2007

54

Summary: the nuclear terrorist threat

55

	Yes	No
❑ Do terrorists want nuclear weapons?	☑	☐
❑ Is it conceivable terrorists could make a crude bomb if they got the material?	☑	☐
❑ Is there material that might be vulnerable to theft and transfer to terrorists?	☑	☐
❑ Is it likely that terrorists, if they had a crude device, could smuggle it to Moscow, London, Paris, Washington, or New York?	☑	☐

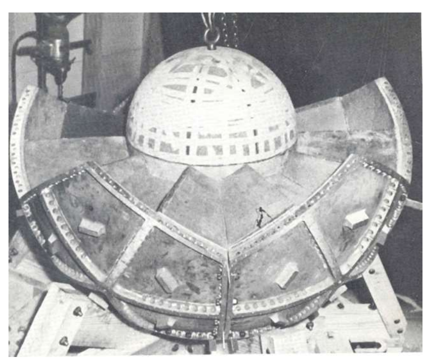
The probability may not be high – but no one would operate a nuclear reactor upwind of a city if it had a 1/100 chance each year of a catastrophic radiation release – risk of a terrorist nuclear bomb may well be higher

55

Implosion-type bombs

56

- ❑ Much more efficient than gun-type bombs
- ❑ Only type that offers substantial yield with plutonium
- ❑ Significantly more complex to design and build
  - More difficult for terrorists, still conceivable (esp. if they got knowledgeable help)
- ❑ Main approaches require explosive lenses, millisecond timing of multiple detonations
- ❑ Some approaches less complex than Nagasaki bomb



Source: Rhodes, *The Making of the Atomic Bomb* (orig. Los Alamos)

56

Hard parts for a crude terrorist bomb

57

- #1: Getting weapons-usable nuclear material
  - Once they have that, 80% or more of the way there
- Others:
  - Processing material into appropriate form
  - Casting and machining (U and Pu difficult materials – esp. Pu)
  - Building explosives, reflector, etc., getting them to work
  - For implosion weapons of the standard type:
    - Precise shaped explosives with very precise timing
    - Need to crush material to denser, more critical form, not flatten it into a pancake
    - Neutron generator to provide shower of neutrons at best moment
  - All this requires an ability to recruit/train skilled personnel, raise money, sustain an organizational effort over a period of time…

Some scenarios might allow some steps to be bypassed

57

Two key potential bomb materials

58

- Highly enriched uranium (HEU)
  - Must separate nearly identical U-235 and U-238 isotopes
  - Nearly all techniques based on their small difference in mass
  - Gaseous diffusion
  - Centrifuges
  - Other: calutrons, laser…
- Plutonium
  - Cause U-238 to absorb neutrons (typically in a reactor)
  - Chemically separate resulting plutonium from the rest (reprocessing)
- A few other isotopes could support explosive nuclear chain reactions, have never been used

None of these materials occur in nature; all are extraordinarily difficult to produce

58

Some (sometimes misleading) terms

59

- *Highly enriched uranium (HEU)*
  - Uranium with at least 20% U-235
  - As opposed to *natural uranium* (0.7% U-235), *low-enriched uranium* (LEU, typically 4-5% U-235), or *depleted uranium* (<0.7% U-235)
- *Weapons-grade uranium*
  - Uranium with ~90% U-235
  - But bombs can be made with material far below weapons-grade
- *Weapons-grade plutonium*
  - Plutonium with ~ 90% Pu-239
  - As opposed to *reactor-grade* plutonium (much less Pu-239) – contained in spent fuel from typical nuclear power reactors
  - Weapons-makers prefer weapons-grade plutonium, but reliable, effective weapons can also be made with reactor-grade plutonium (once reprocessed from spent fuel)

59

Reactor-grade plutonium is weapons-usable

60

- Higher neutron emission rate:
  - For Nagasaki-type design, even if neutron starts reaction at worst possible moment, "fizzle yield" is ~ 1kt – roughly 1/3 destruct radius of Hiroshima bomb – more neutrons won't reduce this
  - Some advanced designs are "pre-initiation proof"
- Higher heat emission:
  - Various ways to deal with – for example, plutonium component can be inserted into weapon just before use (as in early U.S. designs)
- Higher radiation:
  - Can be addressed with greater shielding for fabrication facility
  - Last-minute insertion of plutonium component again

Reactor-grade plutonium is <u>not</u> the <u>preferred</u> material for weapons, but any state or group that can make a bomb from weapon-grade plutonium can make one from reactor-grade

60

The amounts of material required are small

61

- For simple "gun-type" bomb (with reflector): ~ 50-60 kg of HEU (Hiroshima bomb was 60 kg of 80% enriched material)
  - Fits in two 2-liter bottles
- For 1st-generation implosion bomb:
  - ~6 kg plutonium (Nagasaki)
  - ~ 3x that amount of HEU

The size of the plutonium core for the Nagasaki bomb
Source: Robert del Tredici

61

What's true? Reasons for skepticism about the nuclear terrorism threat

62

- States have had great difficulty getting nuclear weapons, surely it would be harder for terrorists
  - Hardest part for states is making the nuclear material – 90% of Manhattan Project
  - Making safe, reliable weapons that can be delivered by missile or aircraft is *far* harder than making crude terrorist bomb
- Terrorist attacks are mostly not very sophisticated
  - But there is a spectrum – some terrorist groups *have* used sophisticated explosive designs
  - Significant numbers of well-trained engineers and scientists have worked with terrorist groups
- Greatly weakened al Qaeda could not organize a nuclear bomb effort
  - Killing, capture, disruption of much of top leadership *does* reduce the risk – but modest cell far from the drone strikes could still be pursuing a nuclear effort

62

What's true? Reasons for skepticism about the nuclear terrorism threat (II)

63

- U.S. intelligence has exaggerated terrorist threats – including in the lead-up to war in Iraq
  - Absolutely correct – skepticism justified. *But* notable that *both* George W. Bush and Barack Obama identify nuclear terrorism as greatest threat to U.S. national security
  - Wide range of other countries (both nuclear weapon states and non-nuclear-weapon states) have reached similar conclusions
- Terrorists could not plausibly get nuclear material
  - Ongoing seizures suggest danger still exists
  - For most seizures, material was never noticed to be missing --how many other thefts have *not* been detected?
- Terrorists not likely to get state support
  - Probably true – states unlikely to hand such power over to terrorist groups they cannot control
  - But state support helpful, not essential, to terrorist nuclear effort

63

Nuclear terrorism: the good news

64

- No convincing evidence any terrorist group has yet obtained a nuclear weapon or the materials and expertise needed to make one
  - Despite many claims
- No evidence any state has helped terrorists with nuclear weapons
- Making a nuclear bomb is clearly not "easy"
  - Al Qaeda and Aum Shinrikyo, both sophisticated, well-funded groups, appear to have faced major hurdles
- Overall, threat is probably lower than 10 years ago
  - Many nuclear sites have much better security, or all nuclear material removed
  - Al Qaeda substantially disrupted
  - *But what may be happening without being detected?*

64

Did you know? Real incidents related to nuclear terrorism

65

- Events that have genuinely occurred:
  - A large-scale terrorist attack on a U.S. nuclear weapons base
  - A terrorist attack on a nuclear facility (not yet operational) in which the armed guard force was overwhelmed, terrorists were in control of facility for an extended period
  - More than a dozen real acts of sabotage at nuclear facilities
    - None apparently intended to cause large radioactive release
    - One involved an insider bringing explosives into a nuclear reactor, placing them on the steel pressure vessel head, and detonating them (before the facility became operational)
    - One involved firing a rocket-propelled grenade at a nuclear facility
  - A Russian businessman offering $750,000 for stolen weapon-grade plutonium, for sale to a foreign client

65

Terrorists might be able to get material: The 2011 Moldovan HEU case

66

- 27 June, 2011: Moldovan officials arrest 6 people for nuclear smuggling
  - 4.4 grams weapon-grade HEU seized
  - Smugglers claim to have access to 9 kilograms of HEU, willing to sell for $31 million
  - Smugglers also claim to have access to plutonium
  - Smuggling through breakaway region of Transnistria
  - Russian leader of group and African buyer are still at large (appears to be first case in some time with serious buyer involved)
  - Moldovan officials report that "members of the ring, who have not yet been detained, have one kilogram of uranium"
  - Little is publicly known about specific characteristics or origins of the material, capabilities of the smugglers, identity of the buyer…

66

Terrorists might be able to get material: Widely varying nuclear security

67

- No binding global standards for how secure nuclear weapons or nuclear materials should be
- Pakistan:
  - Small, heavily guarded stockpile
  - But immense threats – potentially huge outsider attacks, corrupt insiders, some with jihadist sympathies
- Russia:
  - *Dramatically* improved security compared to 15 years ago
  - Cooperative upgrades nearly complete
  - *But*, world's largest stockpiles in world's largest number of buildings and bunkers; underinvestment in sustainability; security culture still needs work; regulations weak; widespread insider corruption
- HEU-fueled research reactors
  - ~120 in > 30 countries, some only night watchman, chain-link fence

67

July 2012: Protester intrusion at Y-12

68

- 3 protesters – including an 82-year-old nun – penetrated to the wall of the building where 100s of tons of HEU is stored
- Failings:
  - New intrusion detection system had been setting off huge numbers of false alarms
  - Cameras that could have assessed alarms had been broken for months
  - Guards assumed alarms were false; guards inside building assumed protesters' pounding was construction they had not been told about
- Root causes and lessons learned:
  - Profound breakdown in security culture
  - Difficult problem to keep guards motivated when attacks never happen
  - Gen. Habiger: "good security is 20% equipment and 80% culture"
  - Every organization handling nuclear weapons and weapons-usable materials needs intensive program to assess, improve security culture, regular tests, assessments of real security performance

68

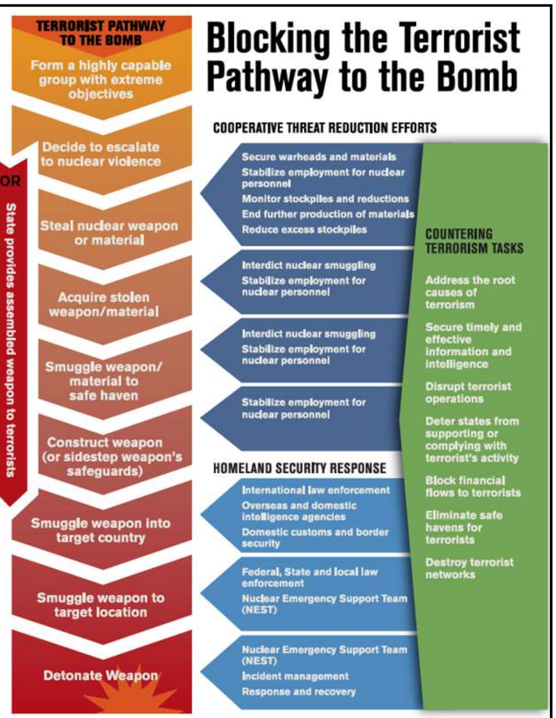
Some recent anecdotes of insecurity

69

- Russia: Gen-Major Victor Gaidukov, commander of a nuclear weapon storage site, fired over accusations of accepting >$300,000 in bribes (2010)
- Pakistan: Brig.-Gen. Ali Khan arrested for ties to Islamic extremists (2011)
- Belgium: Peace activists break into nuclear weapon storage base, spend >1 hour there before being detected and stopped (2010)
- United States: Bomber flies across the country with 6 nuclear weapons on board, no one knows – checks failed (2007)

69

Blocking the terrorist pathway to the bomb



Source: Bunn, Securing the Bomb 2010: Securing All Nuclear Materials in Four Years (2010)

70

70

New steps to reduce nuclear weapons and materials sites

71

- HEU:
  - Still some 120 research and training reactors using HEU fuel or targets – Russia has world's largest share, far more than needed
  - Should agree on target of a *complete phase-out* of civil use of HEU
  - Tons of civilian HEU not currently being addressed – should all be put on a path to elimination
  - Should create new incentives to shift toward international sharing of small number of high-capability, LEU-fueled reactors (or accelerators), shut down remainder. IAEA estimate: ~80% of current reactors not needed
- Plutonium:
  - Should agree to end build-up of stocks, limit number of sites
- Military stocks
  - Need new initiatives to consolidate and reduce these as well
  - U.S. saving hundreds of millions a year on safety and security costs from consolidation in the U.S. complex

71

What would nuclear security success look like?

72

- Number of sites with nuclear weapons, HEU, or separated plutonium greatly reduced
- All countries with HEU, Pu, or major nuclear facilities put in place *at least* a "baseline" level of nuclear security
  - Protection against a well-placed insider, a modest group of well-trained and well-armed outsiders (able to operate as more than one team), or both outsiders and an insider together
  - Countries facing higher adversary threats put higher levels of security in place
- Strong security cultures in place, focused on continual improvement, search for sustainable excellence
- Measures in place to confirm strong security performance
  - Effective regulation, inspection, enforcement
  - Regular, realistic performance tests – including "red teams"
  - Independent, international review – becoming the norm

72

Essential elements of an "appropriate effective" physical protection system

73

- A *design basis threat* reflecting today's threats
- Effective *regulation* requiring all facilities with potential bomb material or posing a catastrophic sabotage risk to have security capable of defeating the DBT
  - Backed up by inspections, and enforcement
  - Ideally including *realistic tests* of the system's ability to defeat outsider and insider threats
  - Effective *control and accounting* of nuclear material
- A strong *security culture*, to ensure that all relevant staff understand the threat and the importance of security
- *Police and intelligence* efforts focused on ensuring that nuclear conspiracies will be detected
- *Regular review and adaptation* to ensure the system adapts to changing threats and opportunities

73

The international nuclear security framework is insufficient

74

- Binding agreements
  - 1980 Physical Protection Convention and 2005 Amendment
    - Parties must have a rule on nuclear security – but what should it say?
    - 2005 Amendment not likely to enter into force for years to come
  - 2005 Nuclear Terrorism Convention
    - All parties to take "appropriate" nuclear security measures -- unspecified
  - UNSC Resolution 1540
    - All states must provide "appropriate effective" nuclear security -- unspecified
- International recommendations
  - IAEA "Nuclear Security Series," especially INFCIRC/225
    - More specific, but still quite general – should have a fence with intrusion detectors, but how hard should they be to defeat?
    - Compliance voluntary (though most countries do)
- Technical cooperation and funding
  - Nunn-Lugar, comparable programs
  - Global Partnership
  - Secrecy, bureaucracy often make cooperation difficult

74

The international nuclear security framework is insufficient (II)

75

- Cooperative frameworks
  - Global Initiative to Combat Nuclear Terrorism
    - 82 nations participating
    - Helps to convince countries of reality of threat
    - Sharing of experience, best practices, capacity-building
    - Modest focus on upgrading nuclear security
  - Proliferation Security Initiative
    - Unlikely to stop smuggling of suitcase-sized items
  - Nuclear Security Summit process
    - Bringing together leaders from ~50 countries
    - Commitment to secure all vulnerable nuclear material in four years
    - Vague group commitments – more specific national commitments
- The IAEA role
  - Developing recommendations, peer reviews, assistance, data
    - All voluntary, largely limited to non-nuclear-weapon states

Many tiles in the mosaic – but is it yet a beautiful picture?
No common baseline of nuclear security for all Pu and HEU

75

Nuclear security is the foundation for the three pillars of the NPT

76

- Disarmament:
  - Nuclear weapon states will not disarm if insecure nuclear material could allow other states or terrorist to rapidly get nuclear weapons
- Peaceful uses:
  - Nuclear energy will not gain needed support unless people are confident that it is safe and secure
- Nonproliferation:
  - Efforts to stop the spread of nuclear weapons will not work if Insecure nuclear material offers states or terrorist groups a rapid path to the bomb

In all these areas, nuclear security is important to the security of all countries around the world

76

Belief in the threat – the key to success

77

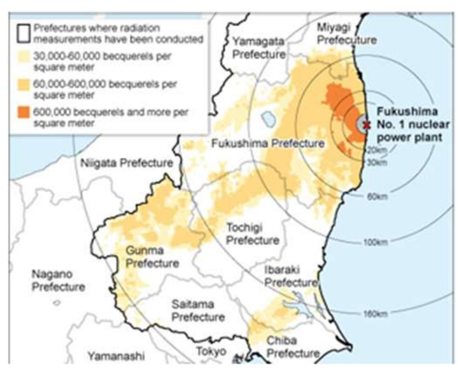
- ❑ Effective and lasting nuclear security worldwide will not be achieved unless key policymakers and nuclear managers around the world come to believe nuclear terrorism is a real threat to *their* countries' security, worthy of investing their time and resources to address it
- ❑ Steps to convince states this is a real and urgent threat:
  - Intelligence-agency discussions – most states rely on their intelligence agencies to assess key security threats
  - Joint threat briefings – by their experts and our experts, together
  - Nuclear terrorism exercises and simulations
  - "Red team" tests of nuclear security effectiveness
  - Fast-paced nuclear security reviews – by teams trusted by the leadership of each country
  - Shared databases of real incidents related to nuclear security, capabilities and tactics thieves and terrorists have used, lessons learned

77

Terrorists have also considered sabotage of major nuclear facilities

78

- ❑ al Qaeda senior leadership has explored the possibility of sabotaging nuclear facilities
- ❑ Chechen terrorists have threatened and planned attacks on nuclear facilities
- ❑ Fukushima showed that destroying both main and backup cooling can lead to major release, create widespread fear



Source: Asahi Shimbun, from MEXT

78

The threat of nuclear sabotage

79

- Most nuclear power plants protected by security forces, containment vessels, and redundant safety systems
- *But,* levels of security vary widely:
  - Some reactors have no (or few) on-site armed guards
  - Few civilian facilities are designed to cope with 9/11 threat -- multiple, coordinated teams, suicidal, well-trained, from a group with substantial combat and explosives experience
  - Some reactors do not have Western-style containments, few redundant safety systems
- *If* attackers could successfully destroy multiple safety systems, reactor could melt down, breach containment, spread radioactive material – as at Fukushima
- Similarly, *if* attackers could successfully drain the water from a densely packed spent fuel pool, real risk that fuel could get hot enough to catch fire -- potential Chernobyl-scale disaster

79

The threat of "dirty bombs"

80

- Dirty bomb could be very simple -- dynamite and radioactive material together in a box
  - Other simple means to disperse radioactive material more effective
- Dangerous radioactive sources in use for valuable civilian purposes in hospitals, industry, agriculture
  - Even large sources often have minimal security
- "Weapons of mass disruption" – not mass destruction
  - Would cause zero to a few near-term radiation deaths, potentially a few hundred long-term cancer deaths (undetectable against natural cancer background)
  - *But,* fear of anything "radioactive" could create panic
  - Expensive, disruptive – potentially many blocks would have to be evacuated, cleaned up (possibly 10s of billions in costs)

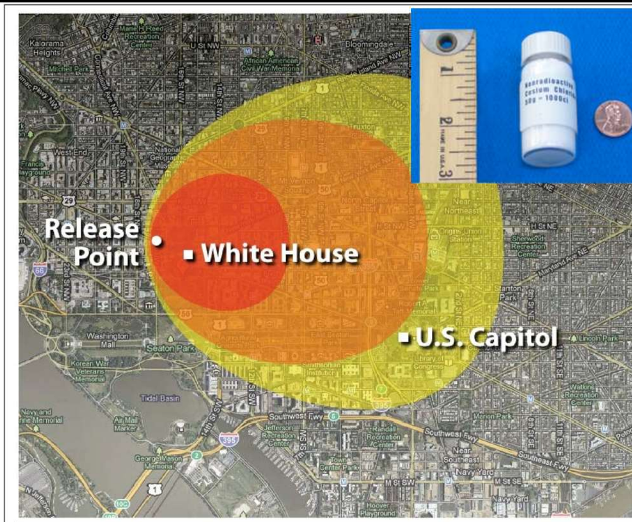
80

Cs-137
“dirty bomb”

81

- Potentially dangerous sources used in hospitals, industry, in almost every country
- Al Qaeda, Chechens have repeatedly considered dirty bomb attacks

Source: Congressional Research Service, modeling by Sandia National Laboratories, 2010



Effects and Actions

	Area km² / mi	Equivalent Dose (rem)	Exceeds relocation PAG for which year:	Population	All Cancers	Fatal Cancers
(red)	2.10 / 0.81	>2.00	First year only	38,000	233	159
(orange)	7.60 / 2.93	>0.500	Any subsequent year	94,700	278	189
(yellow)	13.2 / 5.10	>5.00	50 years (cumulative)	125,000	461	314

Areas and counts are cumulative. RDD detonated at 38.9 N, 77.0 W. PAG: Protective Action Guide

81

Dealing with the “dirty bomb” threat

82

- Better control, accounting, security for radioactive sources:
  - All high-priority sources worldwide should be accounted for, regulated, and have basic security measures (strong locks, alarms, etc.) throughout their life-cycle – IAEA “Code of Conduct”
  - Improved transport security especially needed
  - Retrieve, safely dispose of disused sources
  - Scores of countries worldwide have inadequate controls
- Radiation detection at ports, borders
- Improved capacity to detect, assess, respond to attack
  - Need training, regular exercises, for first responders
  - Develop improved urban decontamination technologies
- Most important: communication strategy to limit panic, tell public how to respond – complicated by past gov’t lies

82

The challenge

83

Lugar Doctrine: war on terrorism will not be won until every nuclear bomb and cache of bomb material everywhere in the world is secure and accounted for to stringent and demonstrable standards

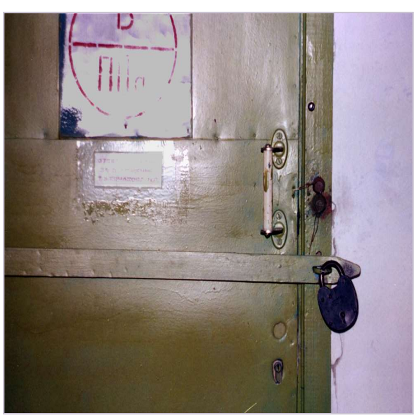
On the day after a nuclear terrorist attack,
what would we wish we had done to prevent it?

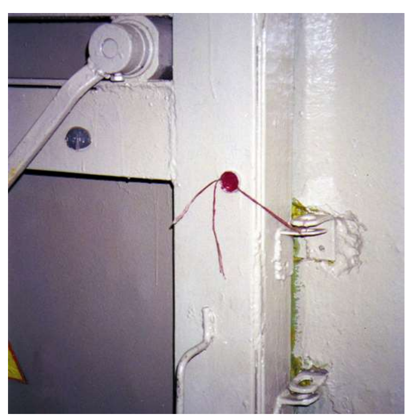
Why aren't we doing it now?

83

Ineffective padlocks and seals for nuclear material in Russia, 1990s

84





84

Antwerp Diamond Center heist, 2003

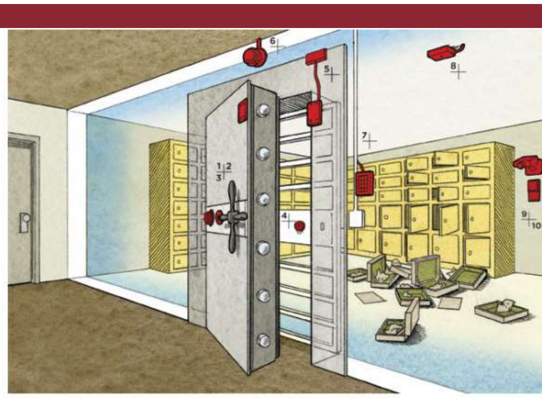
85

Source: Wired

85

Antwerp Diamond Center heist 2003 (II)

86



The Door
1. Combination dial (0-99)
2. Keyed lock
3. Seismic sensor (built-in)
4. Locked steel grate
5. Magnetic sensor
6. External security camera

The Vault
7. Keypad for disarming sensors
8. Light sensor
9. Internal security camera
10. Heat/motion sensor (approximate location)

Source: Wired

86

July 2012: Protester intrusion at Y-12

87

Graffiti from Y-12 Break-In

- 2012: 82-year-old nun and two other protestors enter Y-12 facility
  - Passed through 3 alarmed fences, setting off multiple alarms – no one responded for extended period
  - New instrusion detection system setting off 10x as many false alarms
  - Cameras to allow guards to see cause of alarm had been broken for months
  - Major breakdown in security culture

87

Nuclear security: what are we talking about?

88

- IAEA Definition:

"The prevention and detection of and response to, theft, sabotage, unauthorized access, illegal transfer or other malicious acts involving nuclear material, other radioactive substances, or their associated facilities."

- Focus of this talk is a subset of this broader definition:
  - Security, control, and accounting measures to keep nuclear weapons and the materials needed to make them from being stolen
  - Security measures to keep nuclear facilities from being sabotaged

88

Nuclear security: Why do countries decide to require more or less?

89

- Nuclear security rules, approaches vary widely
  - Among countries
  - Within countries over time
  - Among facilities within a country
- How do these decisions get made?
- What key factors help explain the variations?
- How can this help us understand how to convince states to strengthen nuclear security?

89

The available evidence is problematic

90

- There are no agreed measures to judge whether nuclear security in one place is "better" or "worse" than at another
  - Even "better" or "worse" is incorrect – imposes a one-dimensional spectrum on a multi-dimensional topic
  - Attempts at indices have not adequately captured the issues
  - No agreement on "how much is enough"
- Most nuclear security measures are secret
  - Limits availability of data on current status
  - Limits availability of data on historical evolution
- Most nuclear security changes go largely unnoticed
  - Little if any public debate, reporting in the press
  - In most countries, there is little civil society engagement on nuclear security, so few non-government experts observing

90

But it's clear that many ideas are wrong

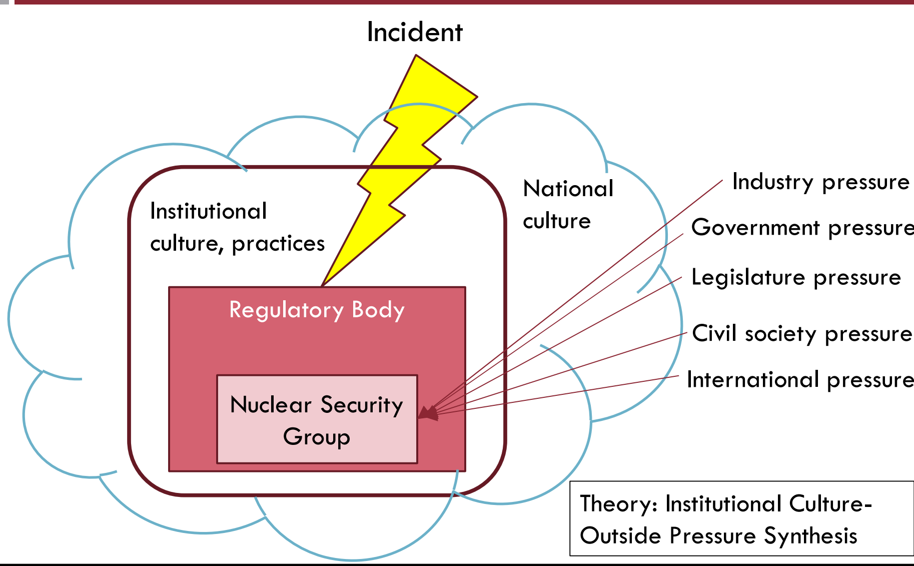
91

- Realist idea that all states with nuclear weapons and weapons-usable material will provide strong security for them is clearly wrong
  - Wasn't true even in the United States for much of the nuclear age
- Rational-actor idea that regulators will set regulations at optimum balance of cost and risk is clearly wrong
  - No data to do this – don't know any of the relevant probabilities
  - Little evidence of serious regulator cost-benefit assessments
- Largely an incident-driven system
  - Complacency about existing security until an incident occurs
  - How system responds to incidents depends on regulatory structures, security culture, and more…

91

Reactions to incidents are modulated by institutional and national culture, pressures

92



92

Nuclear security: 3 layers of action

93

- Local: At facilities and transports
  - What security measures to prevent theft are actually implemented day-to-day?
  - How well are they implemented?
  - How are staff trained and motivated?
- National: National policy and regulation
  - What nuclear security measures are required?
  - What kinds of inspections and enforcement activities are carried out?
- International: Agreements, initiatives, cooperation
  - What do treaties and international recommendations call for?
  - What are international efforts motivating or helping countries to do?
  - What processes are there for dialogue, making commitments, and tracking progress?

93

National regulation and policy

94

- Various questions countries must answer:
  - What threats should nuclear weapons, HEU, plutonium, and nuclear reactors be protected against?
  - What specific security measures should be required?
  - How should these vary with the type of material, and how hard it would be for terrorists to use to produce a nuclear blast?
  - How much will it cost, and who should pay?
  - How do we strengthen security culture?
  - Who's in charge in the event of a real incident, and how do we ensure different parties involved are properly coordinated?
- Many of these are answered in regulations. Key questions:
  - Are the regulations strong enough that, if followed, effective nuclear security would result?
  - How well are the rules implemented and enforced?

94

National regulation and policy (II)

95

- Strong regulation is crucial to effective, sustainable nuclear security
  - Most nuclear managers will not invest in expensive nuclear security systems unless governments tell them they have to
  - A critical element: the design basis threat (DBT) – the threat nuclear security systems must be designed to protect against
- *But,* a culture only focused on following the rules will not achieve excellence in nuclear security
  - Need a culture focused on continual improvement of security – always looking for ways to find and fix vulnerabilities
  - Requires convincing key managers and staff that the threat is real and effective security is part of their mission (not so easy to do)
  - *Incentives* are a crucial part of the story – how to structure?

95

The international nuclear security framework

96

- Key purpose of *international* and *national* frameworks is to ensure effective *local* nuclear security
  - International accords seek to influence national policies, which seek to influence local action – very indirect effect
- International framework includes many elements – a "regime complex," not a single regime
  - Binding agreements
  - International recommendations
  - Technical cooperation
  - Summits and other high-level discussions
  - IAEA services
  - Requirements of supply agreements
  - Best practice exchanges
- Constrained by complacency, sovereignty, secrecy, politics, bureaucracy, cost…

96

Legally binding international instruments on nuclear security

97

- *Not* the NPT or IAEA safeguards
  - NPT does not require any security for nuclear material
  - "Safeguards" are not about either safety or guarding – inspections to confirm material has not been diverted
- 1980 Physical Protection Convention
  - U.S. originally hoped would be effective, binding global standard
  - Least common denominator: covers ONLY security for material in international transport – and only civilian material (~15% of total)
  - Minimal, vague security requirements
  - Includes extensive legal provisions, requiring all parties to pass laws making nuclear theft a crime and giving them authority to arrest and prosecute or extradite nuclear thieves from elsewhere

97

Legally binding international instruments on nuclear security (II)

98

- 2005 Amendment
  - Covers civilian material in domestic use
  - Extends criminal law provisions to sabotage, other acts related to nuclear theft and terrorism
  - Parties must have a rule on nuclear security and an agency charged with implementing it – but what should it say?
- 2005 Nuclear Terrorism Convention
  - All parties to take "appropriate" nuclear security measures – unspecified
  - Mostly focused on legal response to theft, smuggling, terrorism
- UNSC Resolution 1540
  - All states must provide "appropriate effective" nuclear security and accounting – but no one has specified what this means

98

International nuclear security recommendations and initiatives

99

- International recommendations
  - IAEA "Nuclear Security Series," especially INFCIRC/225/Rev. 5
    - More specific, but still quite general – should have a fence with intrusion detectors, but how hard should they be to defeat?
    - Compliance voluntary (though most countries do)
- Technical cooperation and funding
  - Nunn-Lugar, comparable programs
  - Global Partnership
  - Substantial progress – but varies greatly from site to site, country to country; many security elements can't be much influenced from outside; new measures may not be sustained; U.S.-Russian cooperation cut off
- Best practice exchanges
  - WINS
  - U.S.-Russia-UK, others (largely in past)
  - Little data on implementation, some countries do not participate

99

International nuclear security recommendations and initiatives (II)

100

- Global Initiative to Combat Nuclear Terrorism
  - 85 nations participating
  - Helps to convince countries of reality of threat
  - Sharing of experience, best practices, capacity-building
  - Mostly focused on emergency response, forensics, smuggling… modest focus on upgrading nuclear security
- Proliferation Security Initiative
  - > 70 countries participating
  - Focused on interdiction of proliferation-sensitive shipments
  - Also information sharing, excercises
  - Unlikely to stop smuggling of nuclear material that would fit in a suitcase

100

The role of the IAEA

101

- IAEA develops guidance, offers advice, provides services – but only when states request them
  - Broad range of guidance documents
  - >100 member states now have "Integrated Nuclear Security Plans" agreed or in development
  - IAEA offers nuclear security reviews – especially International Physical Protection Advisory Service (IPPAS) (but only a few a year)
  - IAEA provides countless training programs
  - Manages database of illicit trafficking incidents
  - Helps with HEU removals, recovery of orphan sources
  - Provides limited hardware assistance in some cases

101

The nuclear security summit process

102

- The up side
  - Brought together leaders from 50+ countries and organizations
  - Elevated issue from technical experts to political leaders
  - Transformed international debate – greatly increased international attention, decision moments drove new commitments and action
  - More specific "house gifts" and "gift baskets" – most of the latter now IAEA documents open to all
  - Discussion continuing in Nuclear Security Contact Group
- The down side
  - Consensus process led to vague communiqués that probably did little to drive decisions to beef up on-the-ground security
  - Did not agree on any nuclear security standards or any new nuclear security architecture
  - Momentum fading as summits recede into the past

102

The Trump administration's approach

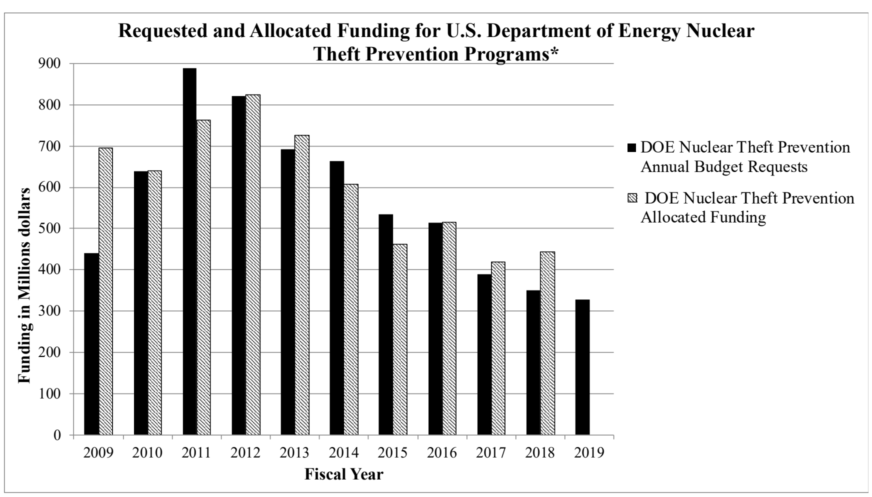
103

- Clearly not as high a priority as in Obama administration
  - Proposed major budget cuts – mostly rejected by Congress
- But Trump team has continued to press for better nuclear security around the globe
  - Continued U.S.-funded nuclear security programs; support for IAEA nuclear security work; participation in Contact Group and other initiatives…
  - Revising nuclear security strategy – broadening some approaches
- As in Obama administration:
  - Work with Russia almost entirely cut off
  - Work with China, India now at modest level
  - Most urgent work with Pakistan completed
  - Nuclear material removals continuing (though some high-priority ones seem politically unattainable…)

103

U.S. nuclear security programs slowing

104



104

We need more effective global governance of nuclear security

105

- Currently we have:
  - No international standards that specify what levels of security nuclear weapons, plutonium, or HEU (or major power facilities) should have
  - No regular international mechanism to build confidence that states are putting effective nuclear security in place
  - No forum for continuing high-level discussion of nuclear security
- Current patchwork of nuclear security agreements, initiatives is clearly insufficient
  - But efforts to negotiate new treaties are unlikely to succeed in a timely way
  - More likely to succeed with political commitments among groups of like-minded states

105

Comparing governance: nuclear safety and nuclear security

106

- International standards
  - Safety: IAEA safety standards and guides in wide range of areas, widely respected and used, fairly detailed (e.g., instructions on how to model potential tsunami threats)
  - Security: IAEA security series recommendations, not standards, less widely followed, not as detailed
- Sharing and learning from experience
  - Safety: Facilities report on incidents, root causes, lessons learned; IAEA/NEA and WANO maintain databases, analyze, and distribute
  - Security: no comparable mechanism
- Peer review
  - Safety: Several varieties of IAEA peer review services; all power reactors members of WANO, agree to accept peer reviews
  - Security: IAEA offers peer review, only a few HEU and Pu facilities have ever had one; no industry peer reviews

106

Comparing governance: nuclear safety and nuclear security (II)

107

- Discussion, identifying next steps
  - Safety: Regular review meetings of the Nuclear Safety Convention; WANO meetings; many others
  - Security: Nuclear security summits – but no other comparable mechanism
- Sharing best practices
  - Safety: Extensive sharing through WANO, IAEA
  - Security: Limited sharing through World Institute for Nuclear Security
- Independent advice
  - Safety: International Nuclear Safety Group (INSAG) publishes annual letters on safety priorities, wide range of analyses and reports; many NGOs providing analysis and critique
  - Security: AdSec provides confidential advice to IAEA, does not publish reports; small number of NGOs involved

107

How nuclear security works: a systems engineering approach

108

- Define what threat system must defend against
- Specify what targets are to be defended
- Design and build a system capable of defending the targets against the threat
- Assess the system – expert judgment, computer analyses, realistic performance tests – can it in fact defeat capable and intelligent adversaries?
- Design and build fixes to identified vulnerabilities, assess again (repeat as needed)
- Operate the system
- Human factor critical: maintain high "security culture," based on awareness of the threat

108

The design basis threat (DBT)

109

- Design basis threat is the set of threats systems are required to be able to defeat:
  - How many outsiders?
  - How many insiders?
  - How many teams?
  - How well trained?
  - How well equipped and armed?
    - Automatic weapons? Night-vision goggles? RPGs? Shaped-charge explosives? Armor-piercing bullets?
  - What kind of vehicles?
  - What kind of tactics and strategy?
  - What motivation? Willing to die?

109

Insider threats are the most dangerous nuclear security problem

110

- The known HEU and Pu thefts, and most sabotages, involved insiders
- People don't want to believe their friends and colleagues could betray the organization
  - Leads to serious lapses in protection against insider threats
- Getting people to report suspicious behavior is *very* difficult
- Often even obvious "red flags" go unreported, unaddressed
- Bunn-Sagan book offers case studies, "Worst Practices Guide" on lessons learned from past mistakes

http://www.belfercenter.org/publication/insider-threats

110

What the security system needs to do

111

- *Detect* – setting off an alarm
  - Example: intrusion detectors on or near perimeter fences
  - Example: active seals on nuclear material container
- *Assess* – what caused the alarm?
  - Example: security cameras at perimeter, critical points throughout the facility
- *Communicate* – "Ten bad guys are breaking in! Go to the north fence to stop them!"
- *Delay* – slow the bad guys down until the cavalry can come over the hill
- *Defeat* – get a response force to the scene fast enough, that is capable enough, to arrest, shoot, etc. the bad guys before the bad guys have an opportunity for catastrophic harm

111

Modeling the layers of the protection system

112

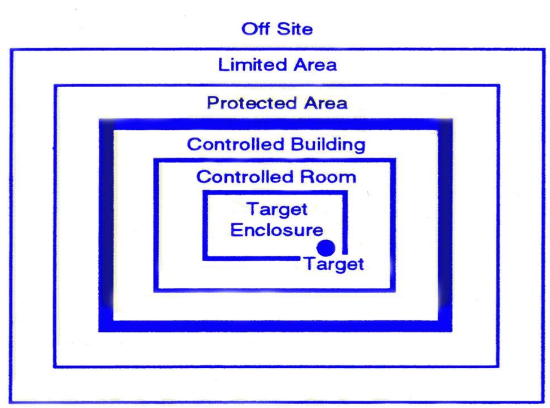


Figure 17–2. Basic Areas At An Example Facility

112

Multiple Possible Adversary Pathways Through Each Layer

113

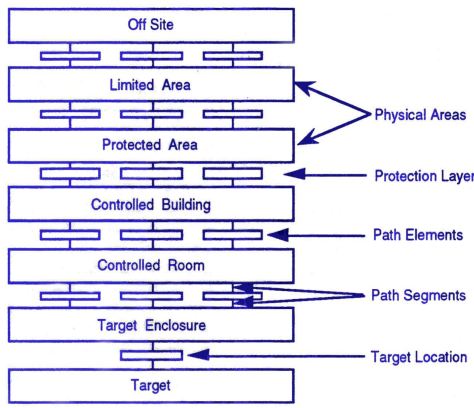


Figure 17–7. ASD Concept

113

Assessing vulnerability assessment

114

- Key issues are similar to those for probabilistic risk assessment – system too complex to predict (and get probability data on) each sequence; unforeseen system interactions and common-mode failures particularly problematic
- Even worse in the vulnerability assessment case, because of intelligent adversaries actively trying to think of things you haven't thought of
- Importance of realistic ***performance testing*** – does the system really protect, when faced with a credible adversary force (and/or insider) trying to overcome it?
- Assessment of ***absolute*** magnitude of vulnerability rarely attempted – never trust a statement that a facility is "secure", always ask "against what, and proven how?"

114

The need for performance testing

115

- Computer vulnerability assessment alone will reveal only the vulnerabilities the assessors think of
- Realistic performance tests – "red team" outsiders attempting to break in, "red team" insiders attempting to smuggle items out – can:
  - Reveal vulnerabilities that require correction
  - Convince higher-ups that more investment in security is in fact needed
  - Provide training for, increase security awareness of, guards and other security personnel
- Regular performance testing required at both DOE and NRC facilities
- Many, many issues – realism, cheating, who tests, how often, etc. – but clearly better than no testing

115

Importance of security culture

116

- If employees don't believe that the threat is real, they won't devote much effort to security measures
- If employees don't believe the security rules are sensible and effective responses to the threat, they won't follow them
- If guards turn off alarms because they are annoyed by the false alarm rate, employees prop open security doors for convenience, and guards patrol without ammunition to avoid accidental firing, even excellent hardware is not enough
- "Good security is 20% hardware and 80% culture."
- Strong security culture is hard to achieve (example: 2012 Y-12 intrusion)

116

Security culture matters: Propped-open security door

117

Source: GAO, Nuclear Nonproliferation: Security of Russia's Nuclear Material Improving, Enhancements Needed (GAO, 2001)

117

Perimeter fences and intrusion detection

118

- Security systems combine:
  - Fences, intrusion detectors, security cameras
  - Typically two fence layers, with clear area between
  - Fences themselves usually provide little delay
  - "Perimeter Intrusion Detection and Assessment System" (PIDAS)
  - Expensive – in U.S., PIDAS costs >$3000/m, $3M for 1 km bunker fence, ~10%/yr for O+M

118

Intrusion detectors – detection

119

- Examples: taut wire, microwave, infrared, etc.
- Each subject to different kinds of false alarms, means of defeating
- Best systems usually have two independent types of sensors
- Guards patrolling perimeter can also serve as detectors
- Guards in guard towers: only ~30% detection probability

119

Cameras, people – assessment

120

- Security cameras traditional – images viewed from central alarm station
- Guards can be sent to assess alarm also
- Adversaries may cause multiple alarms, temporary blinding of cameras, exploit spots with broken cameras…
- Only after assessment suggests attack is underway does timeline for response begin

120

Barriers – delay

121

- Examples: fences, walls, vaults, metal tie-downs
- Many barriers provide few seconds-2 minutes delay against terrorists with shaped charge explosives
- Barriers also help keep adversaries in the open long enough to fire on them
- Newer technologies: sticky foam, cold smoke

121

Protective forces – defeat

122

- Typical arrangement: small force on-site, larger response force some distance away – can they get there in time?
- Response forces must have adequate numbers, armament, training, equipment, fighting positions to defeat adversaries
- Guards in exposed positions likely to be shot – but in bunkers highly effective

122

Protecting against the insider threat

123

- Insider threats are the most important and challenging
  - All nuclear material thefts where the circumstances are known perpetrated by insiders or with the help of insiders
- Insider controls must combine several elements
  - Control the insiders (personnel reliability programs, access control, searches/detectors on entry and exit…)
  - Control the material (tags, seals, cameras, alarms, accurate near-real-time accounting)
  - Control the interactions between the two (two-person rule, monitoring whenever people are near the material)
  - Material accounting is fundamental – especially for stopping slow theft of bits at a time – but uncertainties make it difficult
  - Kinds of accounting and control needed for security are *not* identical to those required for IAEA safeguards
- Comprehensive, multilayered approaches needed

123

Personnel screening and reliability

124

- Access control has limited value unless effective screening of personnel is in place
- Typical approach: background check before hiring (criminal record, terrorist links, financial status, comments from neighbors, co-workers, others)
- Some organizations also use: polygraph (generally ineffective), psychological interviews (probably ditto)
- Continuing checks after hiring also important:
  - Drug and alcohol testing
  - Monitoring of on-the-job performance, reporting of unusual activities
  - Regular monitoring of, e.g., financial status
  - Re-investigation every few years (e.g., every 5 years for U.S. "Q" [nuclear weapons information] clearance)
  - Issue: rapid radicalization

124

Access control

125

- Purpose: allow only trusted insiders into sensitive areas, and only in accordance with rules (e.g., two-man rule)
- Based on something you have (e.g., key), something you know (e.g., password), something you are (e.g., photo, fingerprint, retina scan)
- Guards checking photo IDs minimally effective – IDs readily faked, guards' attention wanders

125

Material control – detecting material removal (ideally in real time)

126

- Security cameras in all nuclear material areas
- Variety of other sensors (as with exterior detectors)
  - Example: Sensor monitors weight of nuclear material in cans on shelf, sets off alarm if weight goes down
- Tags and seals:
  - Example: Active RF seals – instant radio report if tampered with
- Nuclear material detection at doors to key areas (portal monitors)
- Vaults, access control, 2-person rule

126

Material control – tags and seals

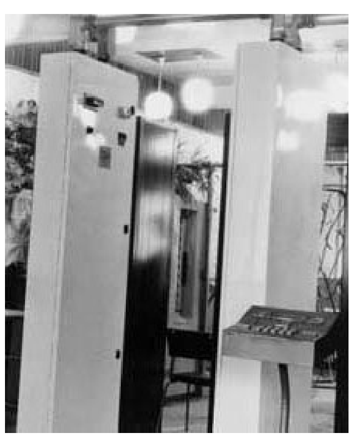
127

- Tags intended as unique identifiers – dummy can't be substituted
- Seals intended to reveal tampering
- IAEA applies hundreds of seals/yr, thousands used in national programs
- Many types – most can be defeated, with varying degrees of difficulty
  - Seal monitored by camera harder to defeat

127

Material control – portal monitors

128



- The best available pedestrian portal monitors are generally effective – though not perfect
- Passive gamma detection
- More difficult to detect material (esp. HEU) in cars, trains, containers
- Many facilities also have metal detectors, X-ray of bags, at least going in (to limit ability to bring in guns or explosives)

128

Material accounting

129

- Purpose: detect removals (after the fact), or confirm that no significant removals have occurred
- Wide range of measurement systems available
- Irreducible uncertainties always exist
- "Protective forces fight the fight, but MC&A tells you who won"

129

Material accounting (II)

130

- Bulk processing facilities are the key nuclear security problem – nearly all known thefts of HEU and plutonium appear to have been from bulk processes

MUF (*M*aterial *U*naccounted *F*or) =

Beginning inventory + Additions to inventory

- Ending inventory - Removals from inventory

- **σMUF** – standard deviation of MUF – is measurement precision
- If MUF > than some threshold level – often **3 σMUF** – accounting system rejects the hypothesis that real MUF is zero, launches investigation
- For item facility (e.g., LWR), MUF=0 unless something is missing

130

Material accounting (III)

131

Tools of Material Accountancy

- *Destructive Analysis* – Take a chemical sample of the material to laboratory for analysis. Highly accurate, but expensive and long delays.
- *Non-Destructive Analysis (NDA)* – Estimate content of U235 or Pu239 by measuring mass, heat, gamma emissions, neutron emissions, transmissivity (e.g., k-edge densitometer), other properties, using portable or on-site equipment. Passive (measure naturally occurring properties, emissions) or active (measure response to pulse of neutrons, gammas, etc.). Less accurate (typically), but far more convenient. DA can be used to calibrate and confirm the accuracy of NDA equipment.

131

International safeguards accounting ≠ to accounting + control for theft prevention

132

- Example 1: Accounting at reprocessing plant
  - May be VERY difficult for international inspectors to confirm that the operator, with the entire resources of the state, is not diverting material
  - May NOT be difficult for the operator to confirm (using knowledge of plant operations, inspection of everything entering and leaving) that small groups of insiders are not removing things
- Example 2: Security measures international inspectors don't care about
  - International inspectors don't care when diversion occurred, who had access at that moment – domestic security people do
  - International inspectors don't care if the workers leave the material out on the tables at night – domestic security people do

132

Example: new accounting and control system at Elektrostal

133

- Major HEU and LEU fuel fabrication facility in Russia
  - Site of multiple HEU thefts in 1990s
- New pilot accounting and control system:
  - Material enters area in sealed canister, accurately weighed
  - Canister can only be opened by worker using his card and passcode – system knows WHO opened the canister and WHEN
  - Canister only opens into glovebox where work is to be done – which automatically weighs the material again
  - Material can only be removed from glovebox into a similar canister, which can only be done using an electronic card and passcode – and it is then measured again
  - Cameras observe the entire area at all times
  - System knows where the material is, and who has access to it, in real time

133

Securing transports

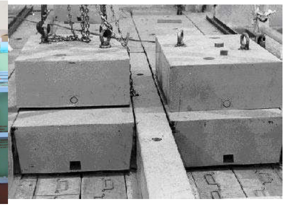
134

- Inevitably more difficult – no fixed barriers for delay, no detection until attack begins
- Nuclear fuel transported in heavy armored casks
- Nuclear weapons in specially designed armored trucks
- Risk can be lowered with investment in security force to accompany
- Some current shipments in some countries lightly guarded

134

"Inherently secure" systems?

135



- Examples: concrete blocks, steel cages
- Less reliance on human factor, security culture
- No need for continuing investments for sustainability
- Only applicable for rarely used material
- Only provide delay – not detection or defeat
- Can be highly effective (and cheap) in concert with other system elements

135

Demonstrated outsider threats

136

- Large overt attack
  - e.g., Moscow theater, October 2002: ~ 40 heavily armed, well-trained, suicidal terrorists, striking without warning
- Multiple coordinated teams
  - e.g., 9/11/01 -- 4 teams, 4-5 participants each, well-trained, suicidal, from group with access to heavy weapons and explosives, >1 year intelligence collection and planning, striking without warning
- Significant covert attack
  - e.g., multiple cases of tunneling into bank vaults without detection
- Use of unusual vehicles
  - e.g., helicopters used in many recent jail escapes
  - e.g., speedboat planned for use in $200M Millennium Dome theft

136

Demonstrated insider threats

137

- Multiple insiders working together
- Often including guards
  - Most documented thefts of valuable items from guarded facilities involve insiders – guards among the most common insiders
  - Goloskokov: guards "the most dangerous internal adversaries"
- Motivations:
  - Desperation
  - Greed/bribery
  - Ideological persuasion
  - Blackmail

A trustworthy employee may not be trustworthy anymore if his family's lives are at risk

137

Some tactics of concern

138

- Deception
  - Example: Thieves dressed as police arrive at Gardner Museum, walk off with priceless Rembrandts
  - Example: Insider pulls alarm, "emergency, everybody out!" and carries material through emergency exit
- Rapid barrier breaching or avoiding
  - Example: throw a carpet over the razor wire in seconds
  - Example: hand-carried explosives can blow through fences, vault doors, even (some) thick walls in seconds
  - Example: tunneling into facility, or flying over barriers in helicopter, hang-glider, etc.
- Conspiracy: multiple insiders, insiders+outsiders
  - Hardest threats to defeat – insiders may include guards (41% of thefts from guarded facilities in one study), security experts

138

Estimating probability of adversary sequence interruption – each pathway

139

Estimate of Adversary Sequence Interruption	Prob. of Guard Comm.		Response Force Time (in Seconds) Mean	SD
	0.95		300	90

Task	Description	P(Detection)	Location	Delays (in Seconds): Mean	SD
1	Cut Fence	0	B	10	3
2	Run to Building	0	B	12	3.6
3	Open Door	0.9	B	90	27
4	Run to Vital Area	0	B	10	3
5	Open Door	0.9	B	90	27
6	Sabotage Target	0	B	120	36
7					
8					
9					
10					
11					
12					

Probability of Interruption: 0.476

139

Estimating probability of adversary interruption: parsing the example

140

- This facility has a response force that takes 300 seconds (5 minutes) to arrive
- But the facility has no ability to detect adversaries cutting the fence – first hope of detection is when they blow through the door of the building
- After that door, it's only 220 seconds to a sabotage
- So, the protection system has less than a 50-50 shot at preventing sabotage on this pathway, against adversaries as capable as those predicted
- Possible fixes: add detection capability at the fence (likely cheapest); put in stronger vaults, etc. to increase delay time after going through door; decrease response force arrival time (e.g., move them closer to facility).

140

Importance of the "human factor"

141

- *Intelligent adversaries* will seek to identify and exploit weaknesses in the system
  - Will actively try to think of things security *didn*'t think of
  - Insiders are particularly difficult to protect against: they know the system and its weaknesses, are trusted by other employees
- *Intelligent employees* will seek to avoid doing things that are inconvenient, boring, that they perceive as unimportant, and that distract from other activities more likely to bring promotion, raises, or pleasure
  - Guards will say they patrolled, checked locks, when they didn't – when the Superbowl is on, they may be watching TV
  - Personnel in general will disregard security rules they think are excessive or useless, and will not behave in the way that system designers may expect – has to be taken into account

141

International accords, recommendations only indirectly affect security on the ground

142

- Goal: ensure that all nuclear weapons, materials to make them, and facilities whose sabotage could cause a major catastrophe are sustainably secured – risk reduced to "as low as reasonably achievable"
- Idea of international initiatives:
  - Hope is that international accords, initiatives will be incorporated in national policies and regulations
  - Hope is that these national decisions will be incorporated in site-level practices
- But there's a long way from what it says in IAEA document to what's actually done at a nuclear facility in Tennessee or Tokai-mura or Seversk
  - On the ground practices determined not only by national policies but by past habits, budget pressures, leadership quality, security culture…

142