HARVARD Kennedy School
BELFER CENTER
FOR SCIENCE AND INTERNATIONAL AFFAIRS

Scenarios of Insider Nuclear Threats – And Steps to Strengthen Protection

Matthew Bunn, Harvard Kennedy School

Nautilus Institute Workshop on Reducing the Risk of Nuclear Terrorism and Spent Fuel Vulnerability in East Asia

21-22 January 2017

belfercenter.org/mta

Nuclear safety and security support nuclear energy growth

- Nuclear energy important to E. Asia's energy future (and those of other countries)
  - Clean, expandable, non-intermittent power
- Public support requires public confidence that facilities will be safe and secure
- Another accident like Fukushima – or, worse, a terrorist attack – could doom prospects for nuclear growth on the scale needed for major climate mitigation contribution
- Resources for safety and security are essential investments in the future of nuclear energy
- Safety and security are inextricably intertwined – often contribute to each other, sometimes conflict

Nuclear theft and sabotage are real dangers

3

- Multiple terrorist groups have sought nuclear weapons
  - al Qaeda's program progressed as far as carrying out explosive tests in the Afghan desert
  - Aum Shinrikyo had substantial effort before 1995 nerve gas attacks
  - Only hints of ISIS interest (extended monitoring of Belgian nuclear official) – but has more $, people, control of territory, ability to recruit globally than the others
- Multiple government studies (in U.S. and elsewhere) have concluded that sophisticated terrorist groups could make a crude bomb if they got the material
- ~20 cases of seizure of stolen nuclear bomb material in public record
- Also multiple cases of actual or planned nuclear sabotage

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

4

- 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

Insider threats are the most dangerous nuclear security problem

5

- 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 – part of an American Academy of Arts and Sciences project

Insider motivations: the radicalized insider

6

- Boughalab is one example
  - Left to fight in Syria, rather than taking action against the reactor
  - Radicalized *after* passing his clearance – within a few months
- Aum Shinrikyo cases highlight the threat from unexpected quarters
  - Members of the police who were Aum members warned the cult of searches, disrupted investigations, may have tried to assassinate head of police investigation
  - Member of Self Defense Forces also involved
- In Japan and ROK, in particular, potential for insiders sympathetic to DPRK

Insider motivations: the coerced insider

7

- Even trustworthy insiders might be coerced – for example if their family is threatened
- Northern Bank case
  - Bank security system required 2 senior officers to open the vault
  - Gang seized the families of 2 senior officers – who helped open the vault, and the gang made off with millions
  - No background check or behavior monitoring program would have highlighted these officers as insider threats
- Coercion by kidnapping family members is a common terrorist tactic
  - *May* have been the intent behind ISIS monitoring of the home of a Belgian nuclear official (not yet clear)
  - DPRK agents could also use coercion

Insider motivations: greed, desperation, disgruntlement

8

- Some insiders take action for money – out of greed or desperation
  - Hirofumi Yokoyama charged with stealing data on 8.6 million consumers, to sell to a credit card fraud ring
  - Korea Credit Bureau insider theft of data on 20 million people
  - Leonid Smirnov: stole 1.5 kg weapon-grade HEU, to care for his family when hyperinflation wiped out his salary (trusted, cleared employee of many years)
- Some insiders are disgruntled, angry with the organization
  - In one database of cyber sabotage cases, >90% came after negative work event, >50% perceived by others as disgruntled
  - Simple steps – listening to employee complaints, sympathizing, correcting valid issues – can greatly reduce disgruntlement

Insider motivations: the inadvertent insider

9

- Some employees undermine security without meaning to
  - Example: John Deutch, when head of the CIA, connected a laptop computer containing highly classified information to the internet
  - Especially important in cyber security: employees clicking on links, downloading software, bringing in USB drives…
  - Countless cases where inadvertent insiders have been important

Insider actions could cover a wide range

10

- Incidents may involve only insiders, or insider and outsiders
- Passive insiders
  - Provide information, but do not take an active part
- Active, non-violent insiders
  - Might do many things, from opening a vault to disabling an alarm to falsifying records to creating diversions to distract security forces
- Active, violent insiders
  - May do all the things active insiders, and use violence – for example disabling a guard at a key post
  - Rarest but most challenging type of insider
- Multiple insiders a particularly challenging problem
- The cyber age multiplies what insiders might do

Example scenario 1: spent fuel pool sabotage

11

- Radicalized insider, seeking to cause a radioactive release
- Waits until fresh, hot spent fuel has just been discharged
- Damages pool gaskets, causing a rapid leak
- Also damages the pumps used to maintain pool levels
- Previously disabled pool level sensor, so that it provided a constant level reading regardless of actual level
- Pool begins to drain, fuel exposed
- Fuel overheats and begins to melt
- High-temperature steam interacts with zirconium cladding, causing spent fuel fire and major release into fuel building
- Hydrogen released from steam-zirconium reaction ultimately detonates, damaging building and causing large release

Example scenario 2: stealing plutonium

12

- Insider works with outsiders to organize theft (perhaps as a result of coercion)
- Removes small amounts at a time from the powder processing area, hides it elsewhere in the facility
- Brings in USB drive that introduces malware that tampers with the accounting records, hiding the losses in larger-than-usual measurement noise
- Arranges for outsiders to pose as contractors to do maintenance on heavy equipment – allowing them to bring in containers which are used to take out the plutonium
- Since the maintenance occurs when the plant is not operating, in an area that does not normally have nuclear material, their equipment is not closely inspected

Scenarios only intended to provoke thought

13

- Measures may be in place that would defeat these particular scenarios – requiring adversaries to choose other pathways
- "Even wildly implausible scenarios get people thinking creatively about security"
- Real thieves or saboteurs would want detailed knowledge of the particular systems they needed to defeat
  - A critical role for insiders

Steps to strengthen insider protection

14

- IAEA recommendations – included in INFCIRC/869 commitment – call for security systems to detect and deter insider adversaries
  - IAEA and WINS have both offered guidance on insider protection
  - Comprehensive insider threat program should include many elements
- Minimizing chances for insiders to succeed
  - Keep material in secure vaults, under constant surveillance
  - Design facilities for maximum passive safety, making it hard to cause a meltdown
  - Minimize plutonium reprocessing or other bulk processing of HEU and plutonium (almost all known thefts have been of bulk material)
- Screening and monitoring staff
  - Background checks before granting access
  - Ongoing behavior monitoring – with strong incentives to report unusual or concerning behavior (difficult, but important)

Steps to strengthen insider protection (II)

15

- Training and motivating staff
  - Nuclear organizations need to build strong security cultures, in which all staff take security seriously – requires focused top-level leadership, strong incentives for security performance
  - Training needs to clearly and vividly highlight the threat, and the relevance of security measures for addressing it – using stories
  - Employee satisfaction also key – treat them well, listen to and respond to concerns and ideas, address bullying bosses
- Controlling, monitoring, limiting access to key material, information, and areas
  - Again, keep material in secure vaults, under constant surveillance
  - Strictly minimize access – and all access should be watched (two-person rule and security cameras)
  - Accounting systems accurate enough to detect both abrupt and protracted thefts, identify when and where they occurred, and who had access at that time

Steps to strengthen insider protection (III)

16

- Limiting, watching all access to the items to be protected
  - Access to materials, information, vital areas only to those who absolutely need it to do their jobs
  - Again, material in secure vaults when not in use, little access to vaults
  - Two-person rule and security cameras watching all access
- Conducting investigations
  - Critical that employees perceive process as fair, reasonable
- Assessment, testing, learning, improving
  - Performance tests – not just of whether accounting or camera systems work, but of whether intelligent insiders can invent ways to defeat the system
  - Vulnerability assessment team regularly looking for weak points
  - Examination of incidents, issues, for lessons learned, ways to improve

East Asian states have done a great deal – but there's more to be done

17

- All states participating in this workshop have made major improvements in nuclear security in recent years – including in insider protection
- But insider protection is inherently difficult
  - Organizations need to find balance between being alert to insider threats and building cooperative, trusting culture for performance
- Hence, need to be always looking for ways to improve
  - International cooperation – including among East Asian states – can help in sharing ideas, approaches to common problems
- Simplest, cheapest risk reduction: store spent fuel in dry casks, rather than storing it in pools or reprocessing it

As with nuclear safety, the goal must be continuous improvement toward excellence in nuclear security performance

Further Reading and Background Material

18

- *Preventing Nuclear Terrorism: Continuous Improvement or Dangerous Decline?* (2016) : http://belfercenter.ksg.harvard.edu/files/PreventingNuclearTerrorism-Web.pdf
- *The U.S.-Russian Joint Threat Assessment of Nuclear Terrorism*: http://belfercenter.ksg.harvard.edu/files/Joint-Threat-Assessment%20ENG%2027%20May%202011.pdf
- *A Worst Practices Guide to Insider Threats: Lessons From Past Mistakes:* https://www.amacad.org/multimedia/pdfs/publications/researchpapersmonographs/insiderThreats.pdf
- *Nuclear Security Matters:* http://nuclearsecuritymatters.belfercenter.org/
- Full text of Managing the Atom publications: http://belfercenter.org/mta

For additional information…

19

An intelligent adversary fundamentally changes probability estimates

20

- 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

Assessing the risk of theft at particular nuclear facilities and transports

21

- 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

Assessing the risk of sabotage at particular nuclear facilities

22

- 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

Comparing nuclear safety and nuclear security risks: the historical record

23

- 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 almost most facilities there); several seizures may be from same theft – but still, shows rate far too high

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

24

- 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

Attack at Pelindaba, Nov. 8, 2007

25

- 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

Coping with creative, determined, evolving adversaries

26

- 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 (partial):
  - Consider updating, expanding capabilities in the DBT
  - Assign creative team with "hacker" mentality to probe for weak points
  - Carry out realistic tests with unexpected adversary team tactics

Broad range of demonstrated adversary capabilities and tactics: outsider threats

27

- Large overt attack
  - e.g., Moscow theater, October 2002: ~ 40 well-trained, suicidal terrorists, automatic weapons, RPGs, explosives, no 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
- Use of deception
  - Uniforms, IDs, forged documents to get past checkpoints, barriers
- Significant covert attack
  - e.g., Pelindaba attackers disabling intrusion detectors
- Use of unusual vehicles or routes
  - e.g., arrival by sea or air
  - e.g., multiple cases of tunneling into bank vaults

Broad range of demonstrated adversary capabilities and tactics: insider threats

28

- Multiple insiders working together
  - Many cases of theft from guarded facilities worldwide
- 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/corruption
  - Ideological persuasion
  - Blackmail

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

Threats may come from abroad: the Vastbërga heist

29

- September 2009, armed men steal millions from a cash depot in Vastbërga, Sweden
  - Arrived in stolen helicopter
  - Had automatic weapons, custom-built explosives, custom-built ladders
  - Delayed police arrival with "caltrops" to puncture tires on nearby roads, bag that looked like bomb at police heliport
  - Escaped with millions ~30 minutes after the theft began
  - Eluded pursuit by abandoning helicopter, switching to unknown car
  - Gang was ex-paramilitary from Serbia – half a continent away

Threats may come unexpectedly from within: Aum Shinrikyo

30

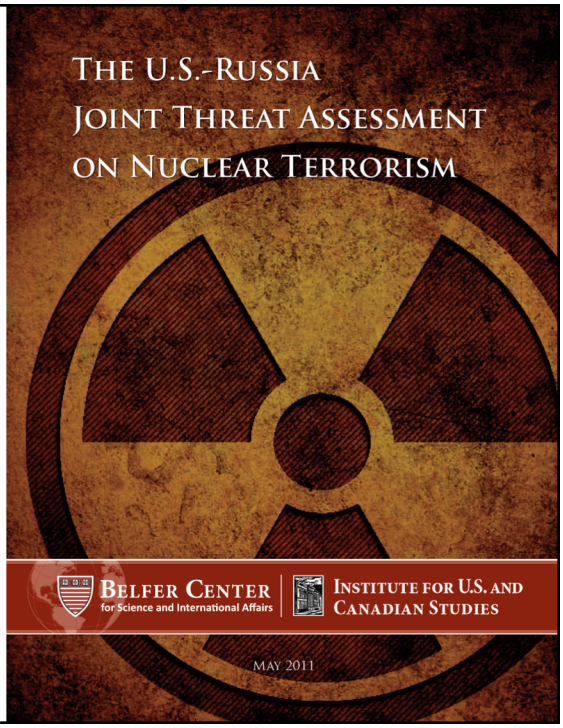
- Japan has long seen itself as a very low-threat country
- But Aum Shinrikyo provides a counter-example
  - Aum had extensive effort to get nuclear weapons
    - Pursued purchase from Russia
    - Bought farm in Australia with U deposits, sought to mine and enrich its own uranium
  - Also had extensive biological program, carried out multiple attempted anthrax attacks (may never have had a deadly strain)
  - Its nuclear, chemical, and biological efforts were unknown to all before its nerve gas attacks in 1995
- Other threats could arise without warning – might focus more than Aum on nuclear material within Japan

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/

31



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

32

- Government studies – in the United States and elsewhere – have repeatedly concluded that a sophisticated terrorist group could plausibly make a nuclear bomb.

  "A small group of people, none of whom have ever had access to the classified literature, could possibly design and build a crude nuclear explosive device... Only modest machine-shop facilities that could be contracted for without arousing suspicion would be required."

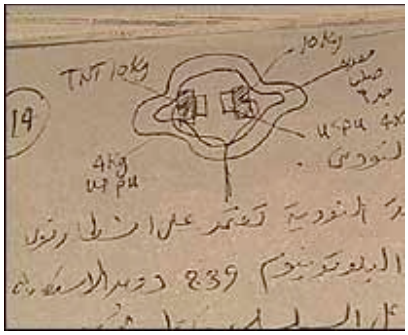
  -- U.S. Office of Technology Assessment, 1977

- U.S. security rules for some types of material based on preventing adversaries from setting off a nuclear blast *while they are still in the building*

Al Qaeda has actively sought to get nuclear bombs

33

- Repeated attempts to purchase nuclear material or nuclear weapons
- Repeated attempts to recruit nuclear expertise
- Focused program that reported directly to Zawahiri
- Reached the point of carrying out crude (but sensible) explosive tests for the nuclear program in the Afghan desert



Source: CNN

Al Qaeda has actively sought to get nuclear bombs (II)

34

- 2001: Bin Laden and Zawahiri meet with 2 senior Pakistani nuclear scientists to discuss nuclear weapons
  - Now-sanctioned UTN network was helping with chemical, biological, nuclear efforts – also offered nuclear weapons technology to Libya
- 2003:
  - bin Laden gets *fatwa* from radical Saudi cleric authorizing use of nuclear weapons against civilians
  - Saudi al Qaeda cell negotiating to buy 3 nuclear devices – if "Pakistani expert" confirms they are real
- 2008: Zawahiri reiterates, elaborates arguments of nuclear *fatwa*

Source: Reuters

Key core al Qaeda nuclear operatives still at large

35

Ayman al Zawahiri  Source: FBI	Now head of the group. Nuclear project reported directly to him.	**Sayf al-Adel**  Source: FBI	Senior al Qaeda operational planner, reportedly personally approved attempted purchase of 3 nuclear bombs in 2003
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.	**"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

North Caucasus terrorists have pursued nuclear and radiological terrorism

36

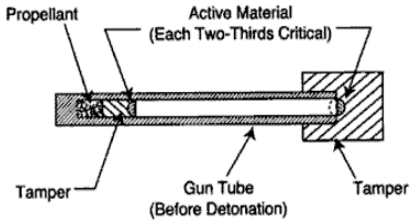
- Multiple cases:
  - 2 cases of teams carrying out reconnaissance at nuclear weapon storage sites – 2 more on nuclear weapon transport trains
  - Repeated threats to attack nuclear reactors – terrorists who seized Moscow theater in 2002 considered seizing reactor at the Kurchatov Institute
  - Repeated 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

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

37

- 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

The scale of the catastrophe

38

- 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

International assessments of the danger of nuclear terrorism

39

"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

Reactor-grade plutonium is weapons-usable

40

- 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

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

41

- 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

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

42

- 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

Nuclear terrorism: the good news

43

- 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?*

Did you know? Real incidents related to nuclear terrorism

44

- 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

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

45

- 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…

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

46

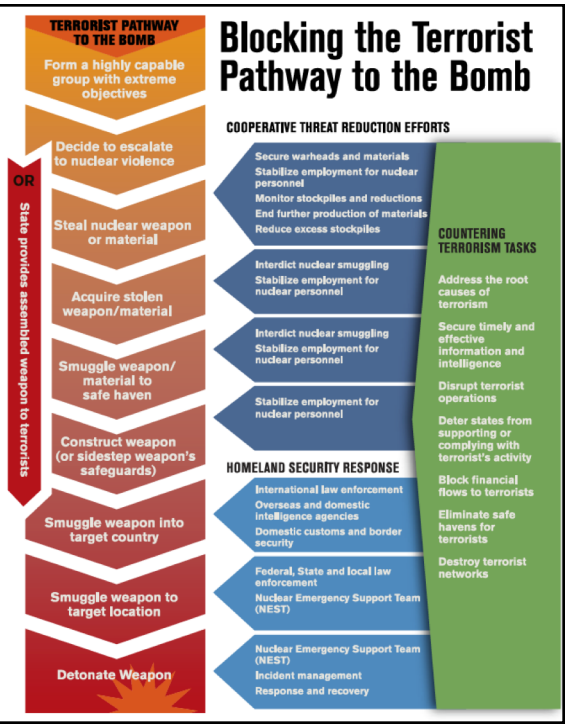
- Nuclear security:
  - North Korea has only a few bombs' worth of plutonium in a tightly controlled garrison state – theft very unlikely
  - Iran has not begun to produce weapons-usable material – has only a small amount of HEU research reactor fuel
- Conscious state transfer:
  - Regimes bent on maintaining 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

Spread of nuclear power need not increase terrorist nuclear bomb risks

47

- 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
- 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
  - Reprocessing does not solve the nuclear waste problem – still need a nuclear waste repository
- Power reactors do pose potential targets for sabotage
  - Sabotage would mainly affect nearby countries, global nuclear industry
  - As with nuclear theft, strong security measures can reduce the risk

Blocking the terrorist pathway to the bomb



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

48

What would nuclear security success look like?

49

- 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

Essential elements of an "appropriate effective" physical protection system

50

- 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

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

51

- 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