HARVARD Kennedy School
BELFER CENTER
FOR SCIENCE AND INTERNATIONAL AFFAIRS

Next steps to prevent nuclear and radiological terrorism -- including actions for Congress

Matthew Bunn
Professor of Practice, Harvard Kennedy School
Capitol Hill Briefing
July 11, 2017
belfercenter.org/managingtheatom

Could terrorists do this to a modern city?

1

Source: *LIFE*, photographer: Bernard Hoffman

Nuclear terrorism is a serious danger

2

- Multiple government studies warn that a sophisticated terrorist group could potentially make a crude nuclear bomb if they got the material
- Terrorist sabotage could cause a Fukushima-scale nuclear accident
- A "dirty bomb" spreading radioactive material could cause expensive disruption, if few deaths
- Terrorist plots suggest possible ongoing interest
  - E.g., ISIS monitoring of senior nuclear official in Belgium

Source: Air Photo Service, Japan

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

3

- 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

Need: a comprehensive program to reduce the risk of nuclear and radiological terrorism

4

- A comprehensive, action-oriented plan
  - Going after the material – secure, minimize
  - Going after the smugglers – find, interdict, impede
  - Going after terrorist groups with nuclear potential
- Resources, authorities to implement the plan
- Someone in charge – with the right support, authorities
- Indicators to judge progress
- Process for learning, adapting, to optimize effectiveness

Today:

- Nuclear security efforts losing momentum after summits
- Intelligence effort focused on nuclear, biological, chemical terrorism small, largely reactive rather than proactive
- Only pieces of comprehensive program in place
- No clear progress indicators, means to learn and adapt

Going after the material

5

- Goal:
  - Effective, sustainable security for all nuclear weapons and weapons-usable material worldwide – includes minimizing stocks, locations
  - Also need better security for nuclear facilities, radiological sources
- Current:
  - Dramatically improved nuclear security over past 25 years
  - But effort losing momentum a year after nuclear security summits
  - U.S. nuclear security programs shrinking, slowing
- Need to revitalize U.S. nuclear security programs
  - From paying for upgrades to convincing states to do more themselves
  - Equally applicable in rich countries and poor countries
  - Will be hard to convince countries to take steps we don't take in U.S.
  - Particularly important targets for cooperation
    - Russia
    - Pakistan
    - India

Going after the material (II)

6

- Revitalized nuclear security programs should focus on genuinely effective implementation in 5 key areas
  - Protecting against the full spectrum of plausible adversaries
    - Are countries defending against everything they should be protecting against?
  - Multilayered defenses against insider threats
    - Insiders have been key to most real nuclear theft, sabotage incidents
  - Focused programs to assess, strengthen nuclear security culture
    - Need all security-relevant staff to be vigilant, aware
  - Realistic vulnerability assessment and performance testing
    - Do nuclear security systems really work, in the face of creative adversaries looking for weak points?
  - Consolidating to fewer sites
    - Can provide better security at lower cost protecting fewer places

Security culture matters: Propped-open security door

7

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

Insider threats are the most dangerous nuclear security problem

8

- 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

Going after the smugglers

9

- The material for a bomb is small and hard to detect
  - Once stolen, could be anywhere
- 1st priority: national police/intelligence teams
  - Trained, equipped to deal with nuclear smuggling cases
  - Proactive – stings, other efforts to penetrate networks
- 2nd priority: nuclear detection
  - Key points – e.g., ports, border crossings that are hard to go around
  - Mobile detection in high-risk areas for smuggling
  - Focus on approaches that can cope with shielding, other adversary efforts to defeat

Source: Los Alamos

Going after the terrorist groups with nuclear potential

10

- Only sophisticated groups with extreme ambitions pose significant nuclear risks, e.g.
  - ISIS (only hints of interest so far)
  - al Qaeda
  - Other groups in future
- Current counterintelligence effort critical but insufficient
- Need focused, proactive intelligence effort to uncover terrorist nuclear plots
  - Targeted team after 9/11 uncovered multiple nuclear, biological, chemical plots
  - Today's effort mostly reactive – waiting for leads
  - Proactive effort, with stings and other techniques, could probe terrorist demand, smugglers' supply
  - Sharing effort internationally – including with Russia – could increase effectiveness
  - If a focused team was unable to find real sources of HEU or plutonium after a sustained effort, likely terrorists would also be unable to do (the "Armageddon Test")

Congress should help launch a reformed effort

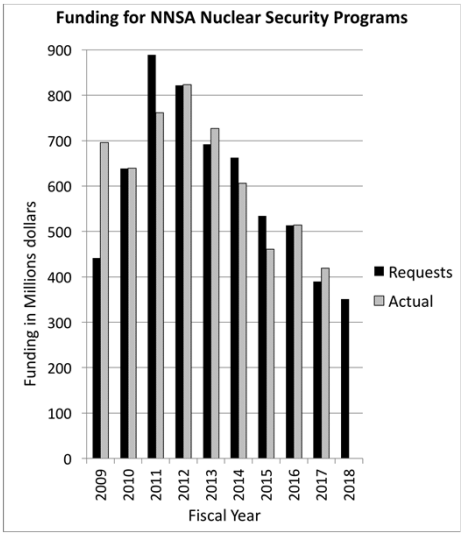
11

- Congress led the way in launching Cooperative Threat Reduction – >2 decades of bipartisan support
- Options:
  - Direct administration to undertake comprehensive, multi-pronged effort to secure nuclear and radiological weapons, materials, and facilities worldwide, take other steps to reduce the risk of nuclear and radiological terrorism
  - Direct, fund a revitalized set of nuclear security programs
  - Direct, fund targeted, proactive intelligence team
  - Require a report on a comprehensive strategy
  - Establish a bipartisan commission to recommend a strategy
- In any of these approaches, important to:
  - Ensure sufficient resources to implement the effort
  - Ensure appropriate leadership, authority
  - Provide regular oversight
    - Have been no in-depth hearings on this threat for years

Congress should provide increased funding

12

- Funding for nuclear security efforts has been cut year after year – now at lowest levels in >20 years
- Trump proposes further cuts
- More funding would be needed for revitalized effort
  - Request is enough for limited current efforts – not for a broader, stronger program
  - In particular, Congress should block proposed 50% cut to "Nuclear Material Removal" and proposed 30% cut to "International Nuclear Security"
- Congress should direct administration to identify funding needed for comprehensive effort



Congress should help launch renewed, reformed nuclear cooperation with Russia

13

- Russian behavior challenges U.S. interests in many areas
  - Sanctions remain justified
  - Some skepticism about cooperation remains justified
- But lack of dialogue, cooperation with world's largest nuclear complex threatens U.S. interests
  - Leads to greater nuclear security weaknesses
  - Denies U.S. experts Russian expertise, test facilities, R&D approaches
  - Leads to less understanding of what's happening
  - Degrades relationships crucial to managing crises as they arise
- United States, Russia, should launch renewed nuclear energy, nuclear security, nuclear safety cooperation – each side paying its own way, sharing ideas, doing joint projects
  - Not U.S. "assistance" to Russia
- Congress should lift or greatly modify NDAA prohibition on contracts with Russian entities – undermines U.S. interests
  - Should also encourage, not restrain, mil-mil contacts

Congress should support the proposal to end the MOX program

14

- Program to use excess U.S. plutonium as mixed oxide (MOX) fuel in U.S. reactors is simply too expensive (~$1B/ton!)
- "Dilute and dispose" provides viable, lower-cost alternative
  - Simple mixing process requiring no new buildings
  - Disposal form safe, reasonably difficult to recover plutonium
  - Still uncertainties on WIPP disposal, but diluted mix could be stored until other repositories become available
- May be possible to amend plutonium agreement
  - U.S. agreed to amend agreement to accommodate changed Russian approach
  - Russian attitude likely determined by broader U.S.-Russian relations, whether other nuclear cooperation being restarted
  - In any case, security benefits of the agreement are real but modest – not worth tens of billions of dollars
  - U.S. policy should focus on maintaining highest possible standards of security and accounting throughout process – in both countries – and verification of process as foundation for limits on fissile material stockpiles

Congress should support minimizing dangerous nuclear materials

15

- Successful effort so far
  - 100s of buildings around the world have been cleared of HEU, Pu
  - >50% of all the countries that once had HEU or Pu have eliminated it
  - But more to be done – especially in Russia
- Support efforts to convert HEU-fueled research reactors and isotope production to LEU that can't be used in a bomb
  - Robust funding for development of new LEU fuels
  - Possible amendment: prohibit FDA licensing of new isotope producers using HEU (mainly a concern about Russia)
  - Fund R&D program to develop LEU fuels for future naval reactors
- Support efforts to work with countries on alternatives to plutonium reprocessing, better ways to reduce Pu stocks
  - Dry cask storage, multinational repositories could change incentives
  - Work with Japan, UK, others on alternatives to MOX
  - Seek to ensure high standards of security and accounting for all plutonium processing

Further Reading

16

- *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
- *Insider Threats:* *http://www.belfercenter.org/publication/insider-threats*
- *Nuclear Security Matters:* *http://nuclearsecuritymatters.belfercenter.org/*
- Full text of Managing the Atom publications: *http://belfercenter.org/managingtheatom*

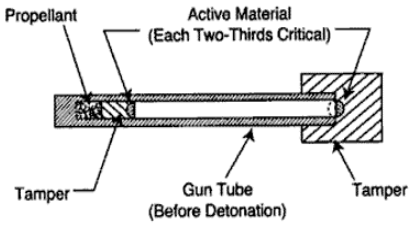
Backup slides if needed…

17

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

18

- 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

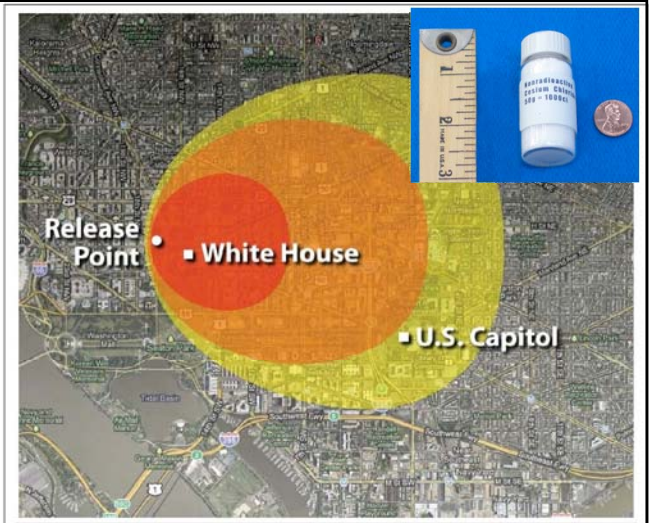
Doesn't take a Manhattan Project -- >90% of the effort was focused on producing nuclear material. And making a crude terrorist bomb is *far* easier than making a safe, reliable weapon

Cs-137 "dirty bomb"

19

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

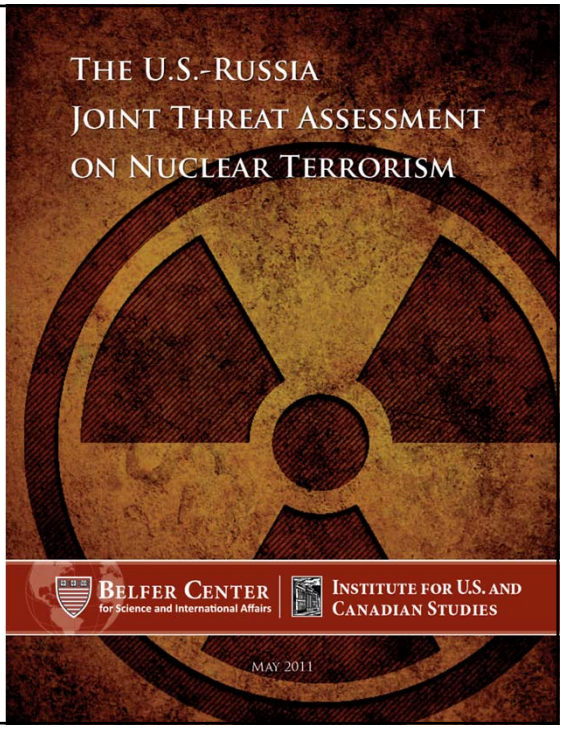
Areas and counts are cumulative. RDD detonated at 38.9 N, 77.0 W. PAG: Protective Action Guide

Not just a U.S. 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/

20



The amounts of material required are small

21

- 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

The insider threat – the biggest issue

22

- All known thefts of HEU or plutonium appear to have been perpetrated by insiders or with insider help
  - ~20 cases well-documented in unclassified literature
  - Many involve bulk material never noticed to be missing until it was seized
- Many factors lead organizations to understate insider dangers
  - Excessive trust in people you know, excessive reliance on background checks, cognitive biases, unwillingness to report concerning behavior…
  - Insiders may understand the security system, how to overcome it
- Widespread insider theft from non-nuclear facilities in Russia
  - Example: insider conspiracy to steal hundreds of items from the Hermitage

The outsider threat – also an issue

23

- Could outsiders attack – or sneak into – a nuclear facility or transport (possibly with insider help)?
  - Example: 2007 intrusion at Pelindaba nuclear facility in South Africa – 2 teams of armed men, likely insider help
  - Countless non-nuclear theft examples all over the world, some with paramilitary-level capabilities and tactics
- How plausible are large, complex attacks like Beslan or the NordOst seizure in today's Russia? Tomorrow's?
  - Large-scale insurgency largely crushed
  - But strong links of some groups to Islamic State, al Qaeda
  - Recent attacks have generally been simpler bombings – but some troubling indicators suggest potential for greater capabilities

Russia's nuclear complex

24

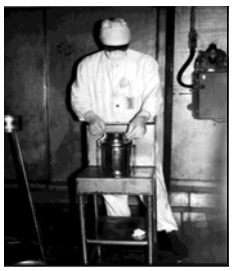
- HEU and Pu in ~200 buildings at dozens of sites
  - Nuclear weapons complex mostly in 10 "closed nuclear cities" – hundreds of tons of plutonium and HEU
  - Major civilian facilities also have HEU and plutonium, from research institutions to large fuel fabrication plants
  - Major bulk processing facilities (biggest insider theft risks):
    - Mayak, Ozersk (closed city, likely site of past theft attempt)
    - Siberian Chemical Combine, Seversk (closed city)
    - Novosbirsk plant (open city, known past thefts)
    - Elektrostal plant (open city, known past thefts)
    - Luch, Podolsk (open city, known past theft)
    - Scale of current processing unclear: Zheleznogorsk, Zelenogorsk, Novouralsk (closed cities)
- Nuclear weapons in >100 bunkers at ~ 40 sites (in addition to deployed ICBMs and SLBMs)
- 34 operating power reactors, huge #s of large sources

Nuclear material in forms that an insider can easily access and remove

25

Source: ORNL

Source: Reuters, from Georgian Interior Ministry



Source: Frank von Hippel

Major nuclear security improvements in Russia – but what's happening now?

26

- U.S.-funded nuclear security upgrades occurred at ~ 90% of Russian weapons-usable nuclear material buildings, nuclear warhead storage sites
  - Also improvements Russia made on its own
  - All the most egregious weaknesses fixed, risk greatly reduced
- But:
  - Some remaining weaknesses (e.g., accounting systems not required to track trends, needed to detect protracted theft)
  - How effective is day-to-day implementation?
  - How strong is security culture?
  - Will they all be sustained?
  - Will Russia do the work of further improvement, to cope with evolving threats, changing technologies, discovery of new vulnerabilities?
- Fundamental issue: complacency ("it's good enough, don't worry")

How does Russia's economic picture affect the risk?

27

- Ongoing recession, low oil prices, devaluation of the ruble
  - Over next several years, will there be recovery, or a 1998-style crisis? What are the probabilities?
  - What effect is the economy having on incentives for nuclear theft? How would that change in the event of a major crisis?
- Major government programs – including Rosatom – facing budget cuts
  - 10% of state employees to be reduced
  - Funding for new reactors cut significantly
  - Other parts of nuclear industry likely facing cuts
- Will budget cuts lead facilities to cut corners on security?
  - Facilities need to find money to meet security rules from general funds – every incentive to cut where possible
  - Nuclear security rules still have significant weaknesses

How does spreading Islamic extremism affect the risk?

28

- What are the chances of one or more insiders being:
  - Self-radicalized? (E.g., Ilyass Boughalab in Belgium)
  - Recruited?
  - Duped or entrapped? (E.g. Clinton jail case in U.S.)
  - Coerced? (E.g., kidnapping family)
- How effective would Russian security services be in identifying such a threat in time?
  - Does the answer vary by type of facility? (Greater counter-intelligence focus on military facilities.)
- Could Islamic terrorist groups put together a sophisticated outsider attack?
  - How effective would Russian security services be in detecting and stopping such a conspiracy?

How does ongoing corruption affect the risk?

29

- Corruption has deeply penetrated the nuclear industry
  - Director and 2 deputy directors of large HEU and Pu facility arrested for corruption
  - Commander of nuclear weapon site relieved of duty for corruption
  - Rosatom has launched anti-corruption program with Transparency International
- Issue may be as much working-level corruption (guards, people with access to material) as high-level corruption that makes news
- How much does engaging in low-level, "normal" corruption affect the chance an insider would participate in nuclear material theft or sabotage?
  - Undermining inhibitions
  - Greed and blackmail both possible

How does the evolving organized crime picture affect the risk?

30

- Substantial organized crime presence in communities with major nuclear facilities
  - E.g., heroin networks in Ozersk and Snezhinsk
  - Recent heroin seizures in both Novosibirsk and Elektrostal
- What are the odds that organized crime groups would consciously get into the business of nuclear theft and smuggling?
- To what degree could nuclear thieves and smugglers make use of organized crime groups without the group's knowing the goods they were helping to smuggle were nuclear?
- To what extent does promixity – organized crime activity nuclear facilities – matter?

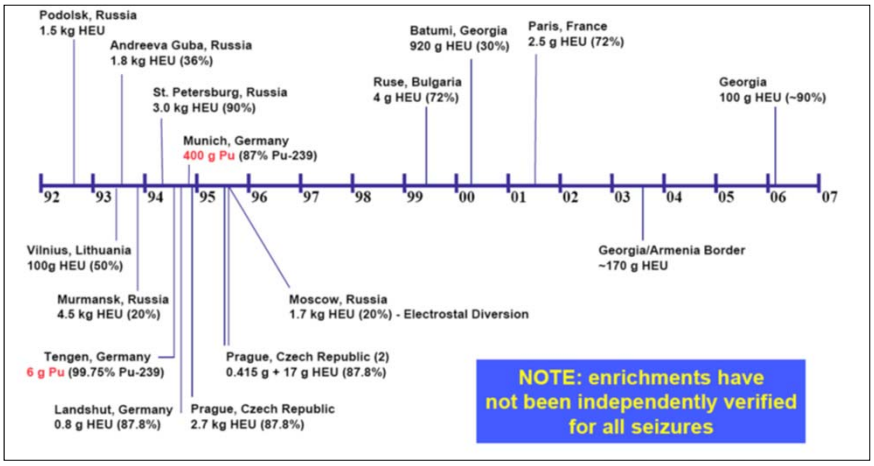
Questions we'd like to answer

31

- How effective are Russia's programs to protect against insider threats?
  - How is the answer changing over time?
- How effective are Russia's programs to protect against outsider threats?
  - How is the answer changing over time?
- How are economic conditions, corruption, violent Islamic extremism, and organized crime affecting insider threats in Russia?
  - How is the answer changing over time?
- How plausible is a substantial, complex, outsider assault on a Russian nuclear facility?
  - How is the answer changing over time?
- What indicators could be tracked to help understand how answers to these questions are evolving?

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

32



Source: Los Alamos National Laboratory, Tom Bielefeld

August 2014: Sabotage at Doel-4 – and a terrorist in the vital area

33

- Insider opened a locked valve, allowed turbine lubricant to drain out
  - Turbine destroyed, reactor down for months
  - $100-$200 million in economic damage
  - Perpetrator, motive still unknown – clearly *not* intended to cause radioactive release
- Investigators found an earlier worker had left to fight for the Islamic State
  - Ilyass Boughalab had passed security clearance to work in the plant vital areas
  - Convicted in absentia of terrorist activities as part of "Sharia4Belgium" terrorist group
- Belgium imposed tougher insider protection rules
  - Better access control, more security cameras in key areas, more use of two-person rule

Does the rise of the Islamic State change the picture?

34

- So far: no clear evidence of a nuclear weapons effort
- But: apocalyptic ideology envisions final battle between "crusaders" and Islamic forces
  - Nuclear weapons could be seen as key part of such a titanic struggle
- Recent extended monitoring of senior official of Belgian site with substantial stocks of HEU a troubling indicator of potential nuclear intent
- If they ever *did* seek nuclear weapons, may be in better position to do so than past terrorist groups
  - More people
  - More money
  - More control of territory
  - More ability to recruit experts globally

Nuclear security: the global picture

35

- **Global stockpiles include:**
  - **~15,000 nuclear weapons**
  - **~ 500 tons of separated plutonium**
  - **~1370 tons of HEU (+/- 125 tons)**
  - **<1/3 of plutonium and HEU is physically in nuclear weapons**
- **Stocks located in 100s of buildings, bunkers, in 29 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

Nuclear security: the global picture (II)

36

- ~20 cases of seizure of stolen HEU or plutonium – most recently in Moldova in 2011
- Can be thought of as global system with 100s of nodes
  - Only as strong as weakest link – failure at any one node could cause horrifying catastrophe
  - No central control over nodes
  - Minimal ability to find and fix the weakest nodes
- Key purpose of all the global agreements, initiatives, summits is to convince states to strengthen nodes within their borders
  - But very little understanding of the factors that motivate change within individual states

Probability of nuclear terrorism may be modest, but consequences are huge – justifies urgent action to reduce the risk

Drivers of nuclear security: the data problem

37

- No agreed measure of nuclear security
  - NTI Index assesses answers to yes/no questions about whether rules of particular types exist
  - Effective nuclear security also depends on *quality* of the rules, and effectiveness of their implementation
  - Experts disagree on the importance of different factors
- Nuclear security measures are largely secret
  - Can get only partial data from published regulations, national reports, conference papers, interviews, site visits…
- Data on change over time is usually unavailable
  - Makes it far more difficult to assess what factors lead to change

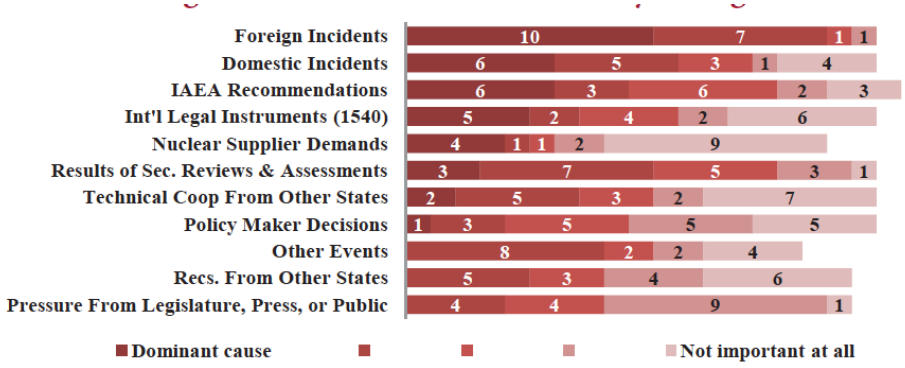
Drivers of nuclear security: Incorrect theories

38

- The realist approach: states will protect nuclear stocks because they are central to their security (e.g., Waltz)
  - Many states transparently failed to do so
- The rational actor approach: states will be provide security at the optimum balance of cost and risk
  - Transparently not the case for much of the nuclear age
  - Most regulators do not attempt to make cost/risk judgments
- Regulation fills public demands, driven by politics
  - Little public interest in or attention to nuclear security
- Full capture: regulation will only serve industry interests
  - Many nuclear security regulations imposed over industry objections
  - But nuclear industry does have outsize influence

Drivers of nuclear security change

39



Source: Bunn and Harrell, *Threat Perceptions and Drivers of Change in Nuclear Security Around the World: Results of a Survey* (2014)

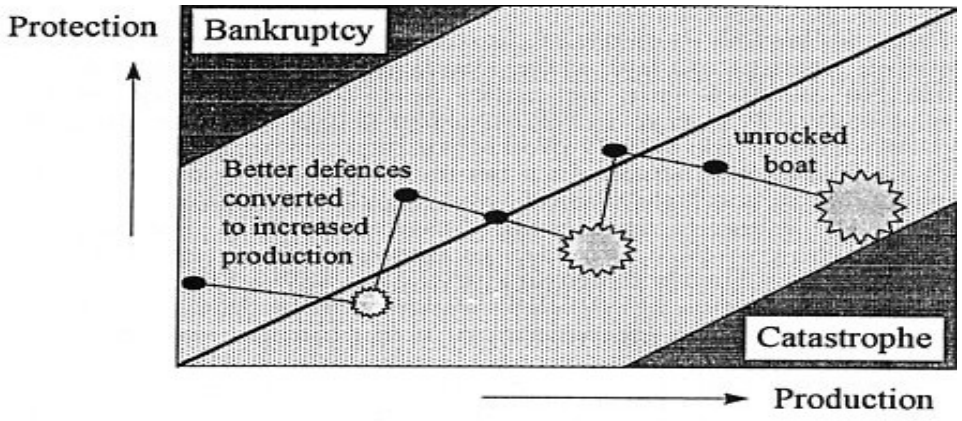
Nuclear security: an incident-driven punctuated equilibrium

40

- **Normal state:**
  - Regulators, operators believe existing security arrangements are sufficient, until there is overwhelming contrary evidence
- **Major incidents drive change – but how much varies**
  - Political, institutional, cultural factors affect how incidents are interpreted, responded to
  - Does a near-miss mean "the system worked" or "we need to fix things so that doesn't happen again"?
- **Policy-makers do not have to wait for incidents**
  - Poor results on inspections, failures in realistic tests can also be "incidents" that drive change
  - International recommendations and reviews are influential
  - In U.S. case, congressional investigations, embarrassing media stories, expert NGOs have played important roles

Navigating the punctuated equilibrium

41



From James Reason, Managing the Risks of Organizational Accidents *(Ashgate, 1997)*

What affects nuclear security on the ground?

42

- Rules & procedures
- Resources
- Training
- Leadership
- Threat perceptions
- Vulnerability perceptions
- Knowledge of best practices
- Incentives
- Organizational and national culture

International discussions and agreements affect these factors importantly, but indirectly

Demonstrated outsider threats

43

- **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., Indian incident with thieves drilling through wall for sources
- **Use of unusual vehicles**
  - e.g., helicopters used in many recent jail escapes
  - e.g., speedboat planned for use in $200M Millennium Dome theft

Demonstrated insider threats

44

- 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

Some tactics of concern

45

- 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

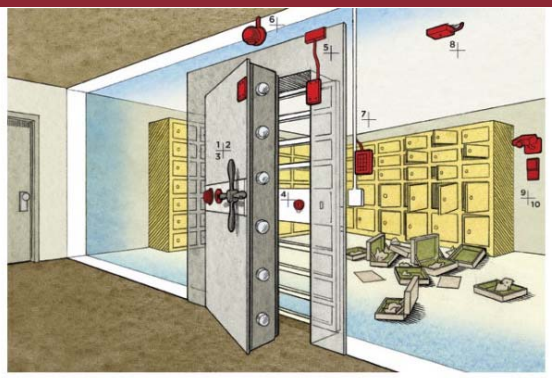
Antwerp Diamond Center heist, 2003

46

Source: *Wired*

Antwerp Diamond Center heist 2003 (II)

47



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*

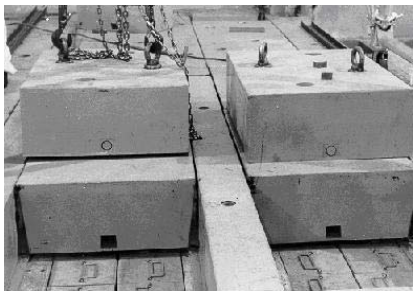
Importance of security culture

48

- 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 approaches to addressing 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 will not provide good security
- "Good security is 20% hardware and 80% culture."
- Strong security culture is hard to achieve (example: recent Y-12 intrusion)

Security measures that minimize reliance on culture

49



Source: Department of Energy

Does equipment influence culture?

50

Source: Department of Energy

How can national authorities influence facility-level security culture?

51

- Very difficult to regulate the quality of security culture (or safety culture) – easier to regulate either:
  - Objectively-measured performance
  - Compliance with rules
- National authorities could require (or encourage, and pay for) operating organizations to take particular steps
  - Regular security culture assessments
  - Programs to address identified weaknesses
  - Could then review quality of each organizations' culture programs, suggest implementation of good practices from other organizations
- Other?

Protecting against the insider threat

52

- 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
- See Bunn & Glynn, 2012, Bunn & Sagan (forthcoming)

Personnel screening and reliability

53

- 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 irregularities, suspicious 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)

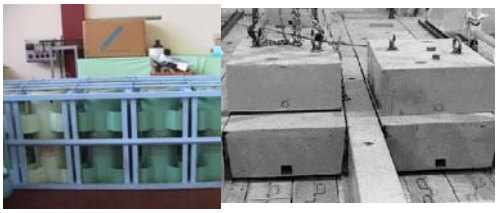
Example: new accounting and control system at Elektrostal

54

- 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 – 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

"Inherently secure" systems?

55



- 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

Could terrorists cause a "security Fukushima"?

56

- Fukushima caused by inadequate preparation and an extraordinary natural disaster
- Reaffirmed that a nuclear accident can cause extraordinary terror, disruption, and cost
- Can be caused by destroying off-site power and backup generators, or destroying cooling system
- Al Qaeda, Chechens, and other terrorist groups have considered sabotaging nuclear reactors

Source: Air Photo Service, Japan

Nuclear safety and security are closely linked – you can't be safe without being secure.

Did you know? Real incidents related to nuclear terrorism

57

- **Events that have genuinely occurred:**
  - **A large-scale terrorist attack on a U.S. nuclear weapons base**
  - **Terrorist teams carrying out reconnaissance at Russian nuclear weapons storage facilities**
  - **An attack on the Pelindaba site in S. Africa (100s of kgs of HEU) by two armed teams**
    - **One team penetrated 10,000-volt security fence, disabled intrusion detectors, went to emergency control center, shot worker there**
    - **45 minutes inside guarded perimeter, never engaged by site security forces**
  - **A terrorist attack on a nuclear facility (not yet operational) in which 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 firing a rocket-propelled grenade at a nuclear facility**
  - **Russian businessman offering $750,000 for stolen weapon-grade plutonium, for sale to a foreign client**

Did you know? Real incidents related to nuclear terrorism (II)

58

- Events that have genuinely occurred:
  - Preliminary explosive tests in al Qaeda's nuclear program
  - Repeated al Qaeda efforts to get stolen nuclear material or nuclear weapons (most recently in 2003)
  - Repeated al Qaeda attempts to recruit nuclear expertise
    - Including bin Laden and Zawahiri meeting with senior Pakistani scientists
  - al Qaeda seeking and receiving religious ruling authorizing nuclear attack on American civilians (2003)
  - Several incidents of al Qaeda considering (but not pursuing) attacks on nuclear power plants
- Good news on nuclear terrorism (*as far as we know*):
  - No convincing evidence terrorists have yet succeeded in getting either materials or expertise needed
  - Risk has likely declined, because of improved nuclear security, large disruptions to "al Qaeda central"
  - Both al Qaeda and Aum Shinrikyo found nuclear to be difficult

Issues for U.S. nuclear security

59

- Y-12 incident reveals major security culture problem
  - May be widespread in the U.S. complex
  - Past problems with sleeping guards, etc.
  - Inadequate attention to assessing, improving the "human factor" in security
- NRC weakening some security rules
  - Exempting reactors using plutonium-uranium mixed oxide (MOX) fuel from Category I security requirements – may exempt MOX fabrication plant as well
  - Considering broader exemptions for plutonium mixed with uranium
  - Threat facilities must protect against weaker than DOEs – even for facilities with tons of weapon-grade HEU metal
- Inadequate attention to insider conspiracies
  - Rules assume with personnel reliability program sites do not have to worry about multiple insiders working together
  - Multiple insiders are common problem in other industries

Issues for Russian nuclear security

60

- Sustainability
  - Government insists sites pay for security themselves – sites with little revenue (e.g., research reactors) may not be able to
- Insider protection
  - Rules don't require tamper-indicating seals that would be very hard to beat, or accounting that could detect slow, "bit-by-bit" thefts
  - Many facilities have emergency doors with no detector or alarm – often open in summer to allow a breeze
  - Widespread corruption and theft of non-nuclear items
- Regulation
  - Regulations still weak in several areas; regulatory agency has limited staff and power
- Guard forces for nuclear material
  - Still heavy reliance on poorly paid and trained conscripts
- Limited realistic testing of security system performance against intelligent adversaries looking for weak points

Some recent anecdotes of insecurity

61

- Russia: Gen-Major Victor Gaidukov, commander of a nuclear weapon storage site, arrested for accepting >$300,000 in bribes (2011)
- Pakistan: Brig.-Gen. Ali Khan arrested for ties to Islamic extremists (2011)
- S. Africa: Two armed teams attack Pelindaba site where 100s of kilograms of HEU is stored, one penetrates 10,000 volt fence, disables intrusion detectors, shoots worker in emergency control center – never caught (2007)
- 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)

Attack at Pelindaba, Nov. 8, 2007

62

- Site with 100s of kgs of highly enriched uranium (HEU)
- Attack by 2 teams of armed, well-trained men, from opposite sides
- 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, establishing regulatory design basis threat