The non-state actor nuclear supply chain

William Tobey and Matthew Bunn
Managing the Atom Project
Harvard Kennedy School
Workshop on "Cooperation to Control Non-State Nuclear Proliferation: Extra-Territorial Jurisdiction and UN Resolutions 1540 and 1373"
4 April 2011
http://www.managingtheatom.org

What has changed?

Compared to 30-40 years ago:

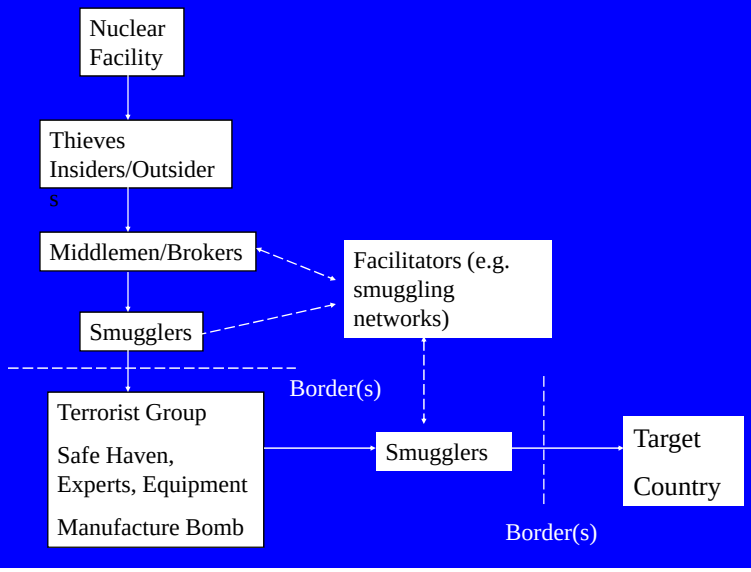
- Emergence of terrorists bent on wholesale, not retail, destruction
- Wide spread of basic nuclear-weapons-related knowledge and information – publications, internet
- Spread of technological expertise
  - Sophisticated parts can be made anywhere where you can set up a precision computer-aided manufacturing machine (e.g., Malaysian plant for Khan network centrifuge parts)
- Globalization
  - Far easier to move people, ideas, money across the world
  - Far easier to put together multinational networks

Two supply chains

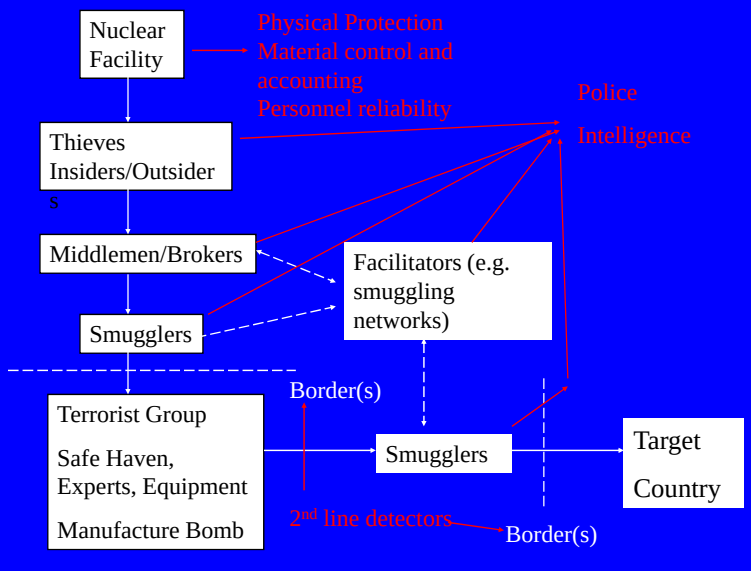
- Weapons-usable nuclear material
  - Typically insider thieves (outsiders, or both, also possible)
  - Brokers, middle-men, smugglers
  - So far, unsophisticated, mostly not connected to organized crime
  - Supply-driven, looking for buyers
  - *Are there more sophisticated actors who aren't getting caught?*
- Nuclear weapons-related technology
  - Sophisticated scientists and engineers are the suppliers
  - Wide range of brokers, front-companies…
  - Often sophisticated strategies to get past controls
  - Demand-driven, from states seeking technology for weapons programs (though networks also proactively peddling wares)

These supply chains may intersect in the future, but have been mostly separate to date

Nuclear materials supply chain



Nuclear materials supply chain



Reducing risk at each step of the nuclear material supply chain

- Preventing theft:
  - Physical protection (equipment, security culture)
  - Material control and accounting
  - Personnel reliability
- Countering smuggling/brokering
  - Police, intelligence (including stings, rewards for information)
  - Detectors at borders
- Countering terrorist plots
  - Address root causes of extreme violence
  - Identify, target groups with nuclear ambitions
  - Prevent large-scale financing
  - Prevent nuclear-expert recruitment
- Countering nuclear delivery – difficult problem

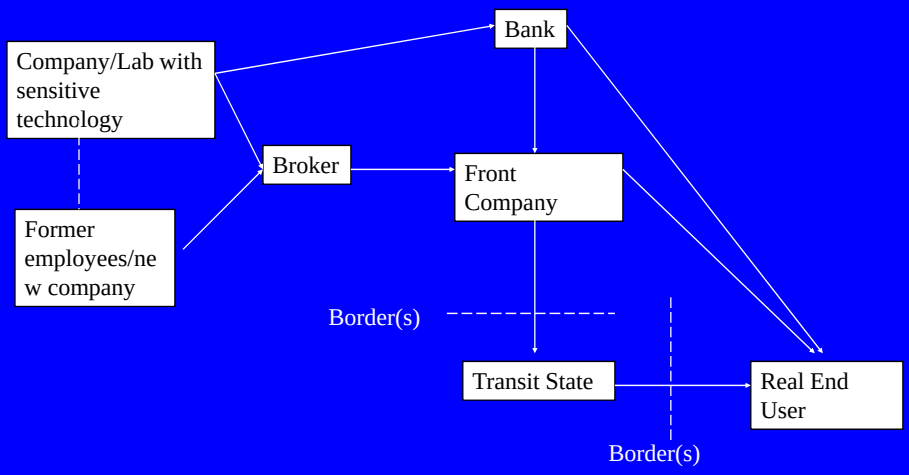
Nuclear material: learning from success and failure

- Failure: ~ 20 known thefts of HEU or Pu
  - All but one insiders, bulk handling facilities
  - All but one not noticed until material was seized
  - Lessons: Strengthen material control and accounting, minimize bulk processing, limit access, institute personnel reliability programs
- Success: seizures
  - Nearly all from (a) luck, (b) participants or others they tried to involve informing authorities; or (c) sting operations
  - Lessons:
    - » Establish police units focused on nuclear smuggling in all key source and transit states
    - » Expand international police and intelligence cooperation
    - » Detectors at borders can push smugglers to riskier routes where they are more likely to be caught – if alternative routes watched

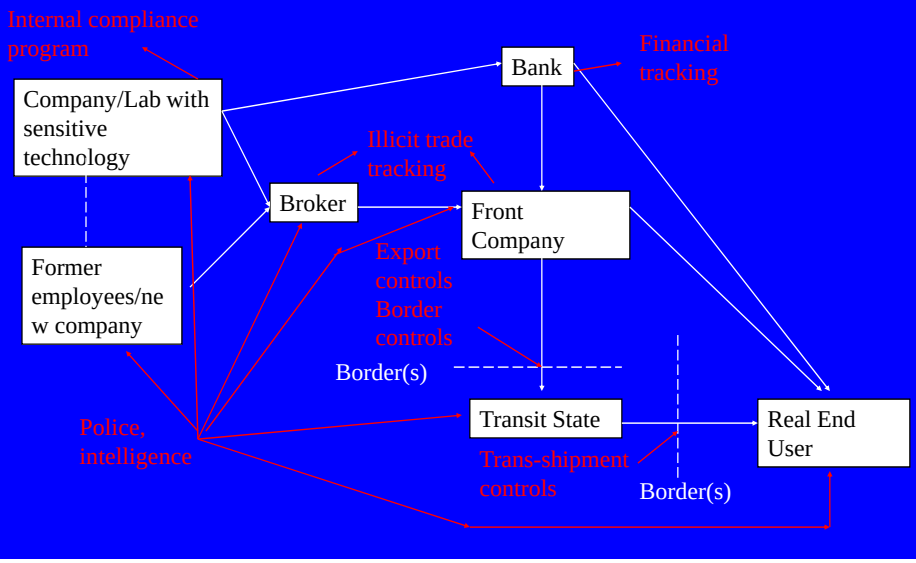
Nuclear material is not hard to smuggle – plutonium box for first-ever bomb

Source: Los Alamos

Nuclear technology supply chain



Nuclear technology supply chain



Nuclear technology: learning from success and failure

- Failure: A.Q. Khan network operates for ~20 years in ~20 countries
  - Lesson 1: all countries need effective export controls, enforcement
  - Lesson 2: companies need effective internal compliance programs
  - Lesson 3: sophisticated global networks are hard to stop
- Success: International police and intelligence cooperation ultimately takes down the network
  - Lesson: critical to establish broad intelligence and police cooperation targeted on black-market nuclear technology networks
- Failure: Minimal or no jail time for network operatives
  - Some cases: laws so weak there were no major violations
  - Other cases: evidence can't be produced in court
  - Other cases: poor sharing of evidence between countries
  - Other cases: weak commitment to enforcement

Corruption is a central enabling element

- Corruption is critical to all these networks – people who, for money, knowingly:
  - Provide nuclear weapons-related material or technology
  - Facilitate theft (e.g., providing inside information on security)
  - Approve illegal exports
  - Allow materials across borders
  - Etc.
- Two campaigns needed:
  - A *nonproliferation culture* campaign – getting people in all key positions to understand that the spread of these materials and technologies is a danger to their countries and to the world
  - A *counter-corruption* campaign – training, transparency measures, penalties, incentives, etc…

Participants in corrupt environments may perceive little risk

Can we deter supply chain participants?

- Increase perceived probability of detection:
  - All the measures just described
- Increased perceived scale of consequences:
  - Put in place "appropriate effective" criminal laws prohibiting participation in such networks, with stiff penalties
  - Renew commitment to enforcement in all countries
  - Strengthen police and judicial cooperation
  - Extra-territorial jurisdiction: ability to punish offenders wherever they may be
    - » Required by Physical Protection Convention, Nuclear Terrorism Convention

This is where 1540, 1373, and extraterritorial jurisdiction contribute to reducing the risk

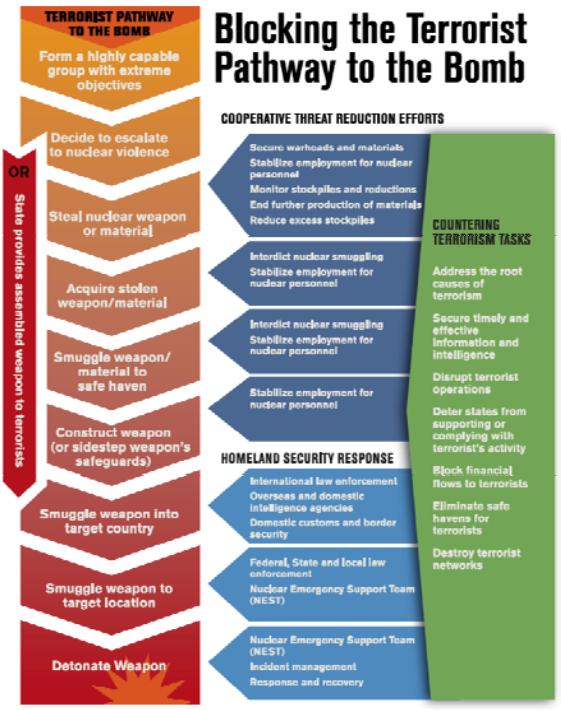
Deterring different participants

- Many participants may be deterred/dissuaded by increased perception that what they are doing is wrong
  - Nonproliferation culture: belief this threatens many
- Different risks may deter different participants
  - Desperate low-level smugglers may require high chance of being caught, high consequence if they are, to deter them
  - Well-to-do engineers may be deterred by more modest risks – though many millions of dollars are at stake in some deals
  - Legitimate companies often strongly motivated by risks to their reputation
  - Once terrorists are smuggling an assembled bomb, or ready-to-assemble pieces, the object(s) will represent a huge amount of effort and money – may be deterred by relatively modest chance of being intercepted and having it all go to waste

Backup slides…

Blocking the terrorist pathway to the bomb

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



Multi-layer defense – focusing on key adversary choke points

- #1 priority: prevent theft of potential nuclear bomb material
  - Once the material has left the facility where it is supposed to be, it could be anywhere, challenge mutiplies a thousandfold
  - Preventing theft is a large but do-able mission – potential bomb material exists in hundreds of buildings around the world (not tens of thousands or millions)
- #2 priority: information/incentive warfare to encourage adversaries to inform, weaken adversary "market"
- Only then does division into land/sea/air interdiction modes become important

Encouraging adversaries to inform

- Known successes in seizing stolen HEU or Pu predominantly *not* from border detectors, but some one informing – often as thieves are trying to find a buyer. "Human factor" – individual who proves unreliable – is the weakest link, both for the good guys and the bad guys
- Hence highest-leverage post-theft point is strengthening the good guys' human factor, weakening the bad guys':
  - Adequate pay for nuclear workers, guards, and effective training (including on dangers of nuclear theft and terror)
  - Toughen penalties for nuclear theft and collaborating with thieves – and widely publicize those penalties
  - Create easy means for anonymous reporting, make sure everyone knows about them – global "WMD 911"
  - Offer substantial, well-publicised rewards for information leading to preventing a nuclear theft, recovering stolen material

Intelligence and police operations to smash nuclear smuggling rings

- Making reliable connections between those who want nuclear bomb material and those in a position to steal it has proved difficult in the past – "market" is weak
  - Difficult to find each other
  - Both buyers and sellers fear stings and scams – difficult to establish *bona fides*, even once initial contact made
- A good defense should seek to make this connection more difficult, catch those exploring this market
  - Demand stings (posing as potential nuclear material buyers)
  - Supply stings (posing as potential nuclear material sellers)
  - Expertise stings (posing as providers and seekers of nuclear expertise)

Expanded police capabilities, int'l police + intelligence cooperation

- Programs should be put in place to ensure that every relevant country has:
  - 1 unit of national police trained and equipped to deal with nuclear smuggling cases
  - All local and other police/intelligence forces informed as to who to call in such a case
  - Access to high-quality nuclear forensics facility to send seized material to
- *Substantial* increase in international police and intelligence cooperation needed on nuclear theft and smuggling – to at least the level of in-depth cooperation now present on counter-terrorism – as threat is transnational
  - In-depth cooperation with Russian FSB in particular difficult but essential to success (some successful FBI, CIA cooperation in other areas under way)

Establishing a global NEST capability

- Nuclear Emergency Support Teams a crucial capability domestically – essential to confirming that hoaxes are not real threats, having at least some capability to find and disable a real threat (if we know where to look)
- Search for remains of Cosmos 954 in Canada proved NEST's ability to operate internationally
- *But*, should put high priority on ensuring all needed arrangements in place for rapid deployment anywhere in the world – including visa exemptions, accords on import of detectors containing radioactive sources, etc.
- May be desirable to undertake NEST cooperation with Russia and other leading nuclear states

Nuclear land/sea/air interdiction – a tremendous challenge

- Length and complexity of borders, huge scale of traffic across them, small size and signature of nuclear material, all make job extraordinarily difficult – some investment desirable, but these layers of defense will always be porous
- 1000s of tons of illegal drugs, millions of illegal immigrants, come into United States every year, despite billions of dollars invested in stopping them
- Even if appropriate training and equipment provided, corruption is a key problem with border and law enforcement forces in many of the most critical countries

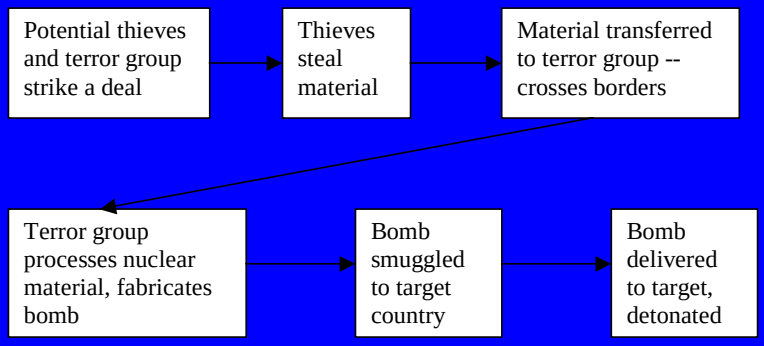
Interdiction: need for a systems approach, focused on adversary adaptation

- Need total *system* design and approach
  - "How well can this detector at this crossing point detect HEU?" is only one small (though important) part of the question
  - Rather, need to understand total system effectiveness, in the presence of intelligence adversaries' efforts to get around it
  - Extensive red-teaming essential, to identify plausible tactics to get around defenses, options for closing those loopholes
- Example: may be possible (and worthwhile) to make it difficult to get an assembled nuclear bomb into the United States in a cargo container. But:
  - Air: what about flying it in on an uninspected Cessna or helicopter?
  - Sea: what about sailing it in in the hold of a yacht?
  - Land: what about bringing ready-to-assemble components in, in backpacks, through wild border areas (e.g., Minnesota "boundary waters")

Interdiction: thinking through adversary responses

- Example: portal monitors installed to scan 100% of containers destined for U.S. at a foreign "megaport":
  - Can the adversaries avoid detection by shielding their HEU, putting it in a shipment that provides shielding, or creates heightened background radiation?
  - Bribe the monitor operator not to notice a "hit," or not to scan one container?
  - Bribe the seal-emplacer to allow an object to be placed in a container *after* it has been scanned?
  - Defeat the seal (open the container, place an object inside, and reseal without this being detected)?
  - Bribe the seal-checker not to notice a tampered seal? (When does this seal-checking occur? How many seals are "naturally" broken?)

One potential terror chain…



Anatomy of a terrorist nuclear plot

- What might a terrorist nuclear plot look like?
  - Might be modest footprint (e.g., a dozen people)
  - Could potentially use facility similar to standard machine shop – may not require equipment whose purchase would raise eyebrows
  - May not require classified information
  - In most cases would require:
    - » Some simple chemical processing (e.g., dissolving stolen material in acid, converting to metal)
    - » Casting metal into desired shapes
    - » Machining cast metal
    - » Well-made and well-designed explosives
  - May use some form of legitimate business for cover (e.g., company manufacturing metal parts)
  - Likely occasional visits and communications with central organization
  - Transport to target country/site if that is not where the weapon is built (may be built to be transported in pieces, quickly assembled)

Crucial roles of police agencies

- Protecting nuclear sites and transports
  - Many rely on police for armed response to theft/sabotage attempts
  - Need in-depth awareness of characteristics, layouts, security plans for all facilities in your area
  - Need regular testing of response capabilities, coordination
- Stopping nuclear smuggling
  - Past successes almost all the result of good police and intelligence work – stings, convincing conspirators to inform, etc.
  - All key source and transit countries need national unit like Georgia's – and other police trained on when to contact them
  - Border forces should receive at least basic training on nuclear smuggling
- Stopping nuclear terrorist plots
  - Will require recruiting specialists, raising large amounts of money, conducting variety of noisy activities – many potential indicators
  - Bomb assembly team may operate in developed country