

Preventing Black-Market Trade in Nuclear Technology

Edited by Matthew Bunn,
Martin B. Malin, William C. Potter,
and Leonard S. Spector



HARVARD Kennedy School

BELFER CENTER

FOR SCIENCE AND INTERNATIONAL AFFAIRS



Next steps to stop an illicit trade

Matthew Bunn (with Martin Malin,
William Potter, and Leonard
Spector)

Sandia National Laboratories

May 17, 2018

An edited volume featuring a who's who of nonproliferation experts

2

- | | |
|----------------------|---------------------------------|
| ❑ David Albright | Current Status and Trends |
| ❑ Ian Anthony | Export Controls |
| ❑ Matthew Bunn | Nonproliferation Culture |
| ❑ Thomasingar | Intelligence |
| ❑ Mark Fitzpatrick | Sanctions and Interdictions |
| ❑ Olli Heinonen | International Organizations |
| ❑ Vladimir Orlov | View from Russia |
| ❑ Robert Shaw | The Role of the Private Sector |
| ❑ Leonard Spector | Enforcement |
| ❑ Justine Walker | Financial Measures |
| ❑ <i>The Editors</i> | Conclusions and Recommendations |

Dangerous black-market nuclear technology trade continues

3

- ❑ All recent nuclear weapons programs have relied heavily on illicit technology purchases
 - Iraq, Iran, N. Korea (at least for enrichment program), Libya, Syria...
 - Despite globalization of technology increasing what can be made indigenously
- ❑ Despite end of A.Q. Khan network, active shopping continues
 - State-directed procurement: N. Korea, Pakistan, India (Iran may resume)
- ❑ Networks are sophisticated, flexible, adaptive, international
 - Tactics continue to change and evolve
 - Response must be equally intelligent and international
 - Ongoing action-reaction cycle: new network tactics beget new controls beget new network efforts to find ways around them

Failures that allowed the A.Q. Khan network to continue for decades

4

Category	Failure
Policy	Failure to act on uncertain information Other priorities
Intelligence	Failure to detect; failure to cooperate (until late)
Export Control	Lack of laws; limited implementation, enforcement
Private Sector Controls	Few companies then had strong controls in place
Law Enforcement	Network participants mainly free (and rich) today (though many spent some time in jail)
Financial Controls	Were not yet in place for nonproliferation
Sanctions	Multilateral sanctions were not yet in place for key countries
Nonproliferation Culture	Weak cultures encouraged supply, or low priority on stopping illicit supply

Nuclear technology: learning from success and failure

5

- ❑ 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

Iran's centrifuges include both indigenous and imported parts

6

A: IR-1 outer casing: aluminum, likely indigenous

B: IR-1 rotor: aluminium, likely indigenous

C: IR-2m rotor: carbon fibre; material imported; fabrication indigenous

D: IR-1 bellows: maraging steel; maraging steel imported; bellows manufactured indigenous

Remainder: likely mix of indigenous and imported



Source: Iran Sanctions Panel of Experts, S/2014/934

Ways around controls on illicit nuclear and dual-use transfers

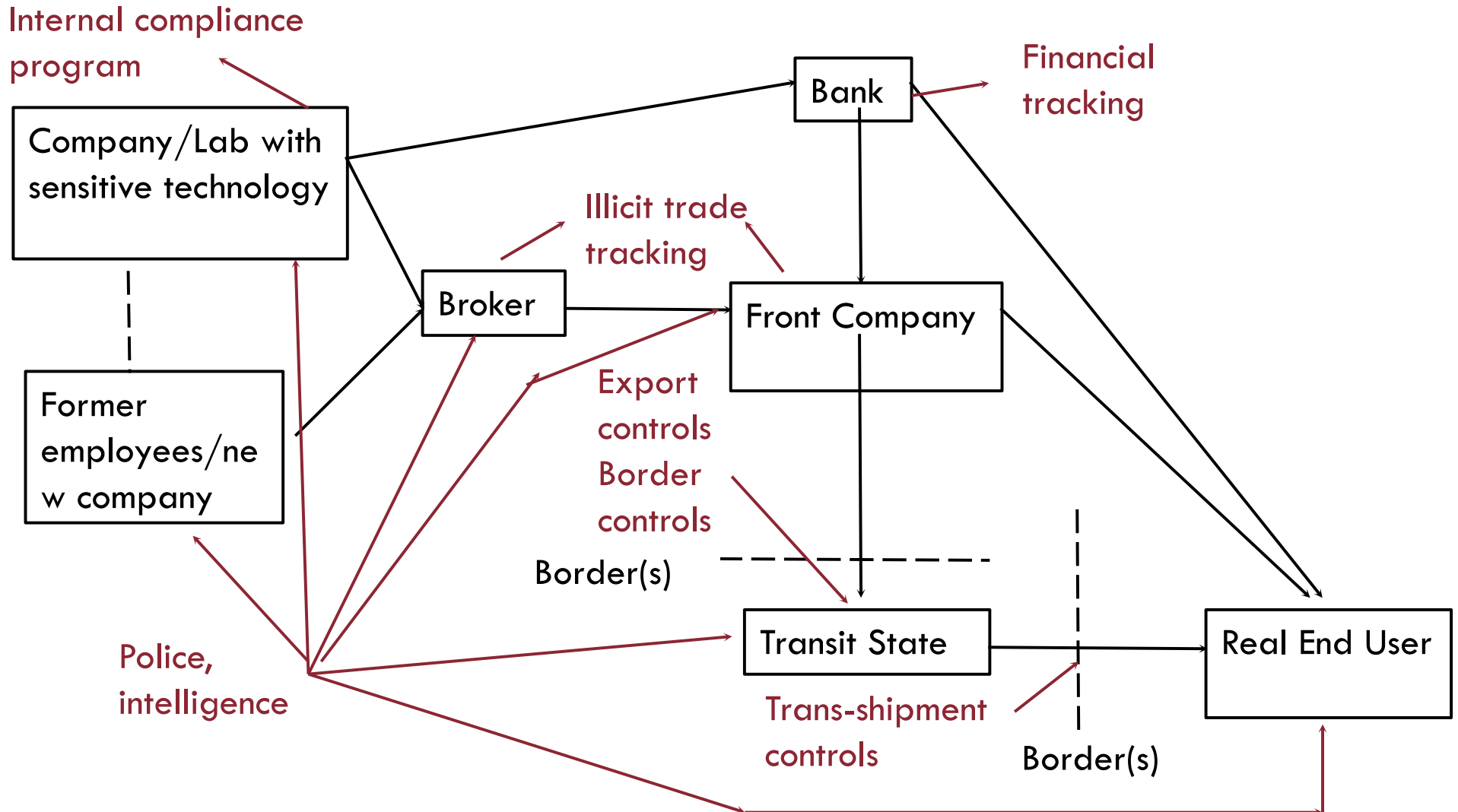
7

Category	Examples
Wear sheep's clothing	False end-use certificates; front purchasers; shell companies...
Go below or around	Buy uncontrolled pieces rather than controlled systems; buy quality just below controls; buy not-yet-controlled tech...
Buy from bad guys	Buy from proliferating states (e.g., N. Korea, Pakistan in past, Iran in future?); Buy from proliferating companies (e.g., Lerch, Griffin, Stemmler, Geiges firms...)
Make yourself	Make centrifuges, plutonium production facilities, weaponization facilities without much foreign supply

- ❑ Procurement networks exploit several or all of these
- ❑ Most illicit transactions now are below-threshold or components of listed items – catch-all controls critical

Nuclear technology supply chain

8



How much progress have existing efforts made?

9

- ❑ Much accomplished in past decade
 - PSI; UNSCRs 1540, 1718, 1737; IAEA; NSG; FATF
 - US targeted and broad economic sanctions (legislation and exec. orders), E2C2 and intel. group, clandestine ops
 - Sanctions by EU and other like-minded states
 - Number of states pursuing n-weapons smaller than in past decades
- ❑ But the problem persists, as do system weaknesses
 - Policy gaps (e.g., some states' unwillingness to act)
 - Intelligence gaps (e.g., poor business-government communication)
 - Export control gaps (e.g., little ability to cope with transshipment)
 - Sanctions and interdiction gaps (e.g., many states and firms have limited implementation ability in face of clever cover stories)
 - Internal corporate compliance gaps (e.g., what to do about employees who leave the firm, such as Gotthard Lerch)
 - International organization gaps (e.g., very limited authority)
 - Financial measures gaps (e.g., limited bank capacity to implement)

Stopping black-market nuclear technology networks: key elements

10

- ☐ Intelligence and information
- ☐ Export controls
 - Including border, trans-shipment controls
- ☐ Law enforcement
- ☐ Interdiction
- ☐ Private sector self-policing
- ☐ Financial controls
- ☐ Targeted sanctions
- ☐ Anti-proliferation and anti-corruption cultures
- ☐ Reducing demand
- ☐ Other?

Limits on the ability to stop illicit nuclear technology transfers

11

❑ Limited knowledge

- Proliferating states and those helping them keep their activities secret — good intelligence is key, but difficult to get

❑ Limited resources

- For enforcement, for awareness, for outreach, for training...

❑ Limited willingness to disrupt legal trade

- Many technologies dual-use
- Measures for licensing, screening, inspecting, etc. all slow down legal trade

❑ Limited international cooperation

- Greater sharing of intelligence, trade data, law enforcement info could help disrupt global networks
- Example: data on license denials and suspicious inquiries

Corruption is a central enabling element

12

- ❑ 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

Major gaps (1)

13

❑ **Weak or absent channels for communication**

- Intelligence agencies to foreign governments, int'l organizations, private sector
- Members of NSG among themselves and to export control bureaucracies internally, and to private sector
- Private sector to and from government and between firms

❑ **No common standards**

- UNSCR 1540 requires “appropriate effective” measures – but no agreed definition, creating international patchwork
- IC and law enforcement using different standards of proof
- Financial institutions have widely varying approaches to when transactions should be blocked

Major gaps (2)

14

❑ Limited authority

- Patchwork of jurisdictions and legal authorities, varying country to country, in some cases:
 - Bank regulators without authority to close banks or block transactions
 - Licensing officials without investigative authority
 - No mechanisms for contesting continued possession and use of illegally acquired nuclear goods
 - Weak sentencing authority for punishing offenders
- Very limited authority for intern'l organizations
 - IAEA, 1540 committee, Interpol, WCO...

Major gaps (3)

15

❑ **Lack of personnel, resources, and organizational capacity**

- No int'l organization responsible for monitoring and disrupting illicit nuclear procurement networks
- IAEA illicit trafficking group, export licensing authorities, customs services, banking regulators all often under-staffed

❑ **Commitment gap/lack of political will**

- Underlying commitment to proliferation goal sometimes uncertain or low priority (e.g., in China)
- Competing priorities in many states for resources and attention (esp. in poor countries)
- Pro-trade factions weaken commitments to controls
- Corruption sometimes defeats control efforts

Recommendations: Overall

❑ Five areas:

- Export controls
- Monitoring
- Intelligence
- Enforcement
- Cooperation with key countries

❑ For each:

- Building capacity
- Improving coordination
- Inculcating nonproliferation culture

Need a major effort, not merely tinkering around edges

Recommendations:

Export controls

17

- ❑ ***Expand efforts to achieve effective export controls worldwide***
 - Additional resources for existing export control assistance programs... including threat briefings... and linking to other border-security goals of recipients
- ❑ ***Establish international peer reviews for national export control systems***
 - Build around 1540 Committee, NSG, or PSI
 - Examine establishment of “international export control task force,” modeled on the Financial Action Task Force

Recommendations:

Monitoring

18

- ❑ ***NSG or PSI should establish an organization dedicated to tracking and disseminating information on suspicious trade that would...***
 - Analyze procurement network activities; report to governments and businesses; develop policy options
 - Formalize suspicious transaction reporting with clear gov't points of contact and protection from liability; establish as industry standard or make mandatory
- ❑ ***Establish an industry Nonproliferation Consultative Group to advise and support governments and international organizations***
 - Advise governments, IAEA, sanctions committees on current illicit shopping patterns, effective approaches to implementing controls, technology trends

Recommendations:

Intelligence + Law enforcement

19

- ❑ ***Encourage close U.S. allies to establish dedicated intelligence teams focused on detecting and blocking illicit trade in nuclear technology***
 - Establish channels to cooperate and share information among these national teams where possible
 - Establish “red teams” as means to find gaps in counter-procurement efforts
- ❑ ***Strengthen enforcement of anti-proliferation laws and stiffen penalties***
 - Increase use of bounties and rewards
 - Update mutual legal assistance arrangements and extradition treaties — and provide such help when needed
 - Establish mechanisms for challenging continued possession and use of illegally obtained goods (as in other areas of illegal international trade)
 - at least to make clear continuing use is a continuing violation

Recommendations:

Cooperation with key countries

20

☐ *Approach China, India, Pakistan, and Russia with initiatives on countering illicit nuclear trade tailored to their specific circumstances*

- China is the key transshipment or source country for most recent nuclear-related transfers to Iran and North Korea
- The United States and China should form a standing Nonproliferation Working Group to address procurement issues and other challenges
- Approach others with specific initiatives

Recommendations more needed if JCPOA unravels

21

- ❑ **Stronger anti-procurement efforts needed if Iran returns to shopping, especially to reduce risk of covert sites**
 - Increased export control assistance, peer reviews, suspicious transaction reporting
 - New organization to track illicit procurement activities;
 - Industry Nonproliferation Consultative Group;
 - Dedicated intelligence teams in allied governments; stronger enforcement efforts and penalties;
 - U.S.-China Nonproliferation Consultative Group
- ❑ **Could help sustain anti-procurement agenda with like-minded states even amid recriminations over JCPOA's fate**
 - Need to convince states to be willing to enforce at least this element of sanctions and controls
 - Could low-capacity states allow others to do end-use verification for them?

Backup slides if needed...

Key conclusions

❑ Intelligence

- Strengthened since 2003
- Improved coordination and international sharing
- Enhanced use of cyber
- But evolving threat, difficult obstacles to wider cooperation, little business-government reporting

❑ Export controls

- Strengthened laws, implementation worldwide (with some exceptions)
- Networks forced to seek below-threshold items
- Catch-all provisions added (NSG and UNSCRs), playing increasing role
- But technology spreading, indigenization growing, evasive strategies still succeeding, developing states have few resources for implementation, China (and others) still pose challenges

Key conclusions (2)

24

❑ Sanctions and interdictions

- Stringent sanctions, increased interdictions *are* hindering nuclear weapon programs
- Broad economic sanctions helping to dissuade states from pursuing this course
- Sanctions can buy time and create incentives for diplomacy, *but* always have gaps and can also spur indigenization

❑ Financial measures

- Asset freezes, denials of access to Western banking system, prohibiting the use of SWIFT, and Financial Action Task Force anti-money laundering measures all disrupting networks
- But networks developing work-arounds (though complexity still inhibits transactions), Implementation by financial institutions spotty in some cases, overbroad in others

Key conclusions (3)

25

❑ Law enforcement

- Can disrupt, shut down networks
- Threat of punishment increases private sector compliance, deters some actors from participating
- But combination of few prosecutions and lenient penalties undermining deterrence; need for increased international sharing, help

❑ Private sector

- New barrier for networks through great increase in due diligence in manufacturing, courier, shipping, insurance, and financial sectors
- But small and medium-sized firms often lack resources to implement rigorous oversight, insider threats remain a serious problem, and technology may be provided by former employees outside the firm's control

Key conclusions (4)

26

❑ IAEA and other international organizations

- UNSC playing major role with passage UNSCR 1540 and Iran/North Korea sanctions resolutions
- But sanctions committees have few resources, rely on member states to provide information
- IAEA has extensive experience in tracking illicit nuclear trade
- But IAEA has no authority to disrupt or punish, most states do not allow direct discussions with firms and provide only limited intelligence, information goes *only* to safeguards department

❑ Nonproliferation culture

- Shared belief in importance of nonproliferation measures increasing in government, research, and private sectors
- But still often weak awareness, and less in small and medium-sized firms and in some countries; competes with other institutional priorities

Can we deter network participants?

- ❑ Increase perceived probability of detection:
 - All the measures just described
- ❑ Increased perceived probability, 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

Can we deter network participants? (II)

28

- ❑ 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