



HARVARD Kennedy School

BELFER CENTER

FOR SCIENCE AND INTERNATIONAL AFFAIRS

Protecting nuclear materials and facilities against the full spectrum of plausible threats

M. Bunn, N. Roth, W. Tobey

Managing the Atom Project, Harvard Kennedy School

IAEA Conference on Physical Protection of Nuclear Material
and Nuclear Facilities, November 13–17, 2017

belfercenter.org/managingtheatom

Effective nuclear security systems must protect against a broad spectrum of adversaries

1

- ❑ Key dilemma for nuclear security
 - States must protect against all realistic threats
 - But should not waste money protecting against unrealistic threats
- ❑ Existing agreements, resolutions, recommendations require effective protection against state's understanding of the threat
- ❑ Recent incidents demonstrate broad range of potential adversary tactics and capabilities
 - Key data for assessing what the design basis threat should be
 - But adversaries learn, adapt, change, so the past is not a fully reliable guide to the future

International instruments call for protection against the state's understanding of the threat

2

- ❑ UN Security Council Resolution 1540
 - Provide “appropriate effective” security for all nuclear weapons and related materials
 - To be truly “effective” security must protect against all the types of theft attempts that might plausibly occur
- ❑ Amended physical protection convention:
 - Provide protection against “the state’s current evaluation of the threat”
- ❑ INFCIRC/225/Rev. 5
 - Protect against a DBT based on a regularly updated assessment of the threat, including all credible information
 - Key IAEA recommendation, so included in the commitments of the Strengthening Nuclear Security Implementation Initiative (INFCIRC/869)

Recent incidents provide lessons on adversary capabilities and tactics

3

- ❑ Recent incidents of theft from or attacks on secured facilities demonstrate a wide range of capabilities and tactics
 - Well-armed, well-trained outsiders, sometimes with military-style tactics
 - Use of insiders (including multiple insiders in some cases)
 - Unusual vehicles to get past some layers of security (e.g., helicopters)
 - Prolonged intelligence collection to understand security system
 - Use of deception (e.g., official uniforms, forged IDs and documents)
 - Use of multiple teams, including to distract/delay response forces
 - Use of cyber intrusions (could be combined with physical theft or attack)
 - Willingness to die in the attack

Example: The Vastbërga heist

- ❑ September 2009, armed men steal millions from a cash depot in Vastbërga, Sweden
 - Arrived in stolen helicopter
 - Had automatic weapons, 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



Source: NTDTV

Insider threats are the most dangerous nuclear security problem

5

- ❑ Most 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>



Cyber intrusions

6

- ❑ Cybersecurity must be a key part of nuclear security protection
- ❑ Cyber means can be used to undermine all of the principal nuclear security measures
 - physical protection
 - material control
 - accountability, and personnel reliability programs.
- ❑ Collecting and sharing of cyber threat information is already taking place in some sectors



Source: cyberaware.gov

The need for expanded sharing of incident information and lessons learned

7

- ❑ It is crucial for both national governments (including regulators) and operators to be aware of the full spectrum of the threat
 - Yet detailed incident information – including the tactics adversaries used, how they defeated the security system, and how security systems could be modified to prevent similar attempts – is rarely shared
- ❑ States should develop approaches to compiling and analyzing such incident information, and sharing it with operators
- ❑ Means should be developed to share such information internationally as well
 - Some information is secret or sensitive
 - A great deal of important information is open-source, or could be shared between cooperating states
 - Example: U.S. sharing about 2012 Y-12 intrusion (should be expanded)

Protecting against a common baseline threat

- ❑ Adversary capabilities and tactics vary from place to place
- ❑ But in a world with terrorists with global reach, there is a need for a common baseline of protection:
 - Weapons-usable nuclear materials and high-consequence nuclear facilities should, at a minimum, be protected against:
 - A modest group of well-trained, well-armed outsiders (able to operate as >1 team), a well-placed insider, and both outsiders and an insider together
 - Cyber threats, including the use of cyber assaults to compromise or confuse security systems to facilitate a physical theft or assault
 - Should be a floor, not a ceiling – countries facing higher adversary threats should put higher levels of security in place
- ❑ States should convene experts to develop such a common baseline – and make a political commitment to implement it

Cooperation to protect against the full spectrum of adversary tactics & capabilities

9

- ❑ International cooperation and commitments can help achieve effective nuclear security worldwide
- ❑ A next step: political commitment to key nuclear security principles – flexible, but specific enough to be meaningful
 - One approach: draw on physical protection, material control, and material accounting goals from US-Russian technical cooperation
 - Most fundamental element of principles should be a commitment to protect against common baseline threat
- ❑ Group of like-minded states might develop principles
 - Initial participants (ideally, most or all of the states with substantial stocks of weapons-usable nuclear materials) could invite other states to join, and offer help in meeting the commitments

Cooperation to protect against the full spectrum of adversary tactics & capabilities (II)

10

- ❑ Obstacles to cooperation to achieve protection against a broad spectrum of adversary tactics and capabilities worldwide
 - Complacency
 - Secrecy (don't want to reveal information about defenses to adversaries)
- ❑ It's possible to build confidence without revealing sensitive information
 - Review of security arrangements by international experts (IPPAS)
 - Confidential information sharing about security requirements, assessment and testing approaches to ensure that they are met
- ❑ IAEA should have a central role
 - Principles could be established in an INFCIRC open to all states, IAEA could help coordinate assistance, reviews on request
 - Military materials security should be addressed outside the IAEA

Ensuring that nuclear security systems will perform as required

11

- ❑ States should have mechanisms for in-depth assessment and realistic testing of nuclear security system
- ❑ INFCIRC/225/Rev. 5 recommends nuclear operators have quality assurance programs
 - Including at least annual force-on-force exercises
- ❑ Genuinely effective quality assurance programs include:
 - Realistic force-on-force exercises
 - “Red teams” to find security vulnerabilities and propose solutions
 - In-depth vulnerability assessment evaluations
 - IAEA should develop guidance and advisory services on how to conduct realistic assessments and performance testing
- ❑ The IAEA, the United States, and other interested parties should work to convince countries to carry out regular, realistic tests

Further Reading and Background Material

- ❑ *Preventing Nuclear Terrorism: Continuous Improvement or Dangerous Decline?* (2016) :
<https://www.belfercenter.org/sites/default/files/legacy/files/PreventingNuclearTerrorism-Web.pdf>
- ❑ “Key Steps for Continuing Nuclear Security Progress” (2016)
https://www.belfercenter.org/sites/default/files/files/publication/%5B3A-1%5D_FUL_574_Bunn.pdf
- ❑ *Insider Threats* (2017)
<http://www.belfercenter.org/publication/insider-threats>
- ❑ *Threat Perceptions and Drivers of Change in Nuclear Security Around the World: Results of a Survey* (2012)
<https://www.belfercenter.org/sites/default/files/files/publication/surveypaperfulltext.pdf>
- ❑ Full text of Managing the Atom publications:
<http://belfercenter.org/mta>