Lecture 4. NUCLEAR AND RADIOLOGICAL TERRORISM: THREATS AND RESPONSES

Course “New Challenges to the Nonproliferation Regime”

Dr. Alexey Ubeevo

Dual Master’s Degree Program in Nonproliferation Studies
Moscow, Fall – Winter 2016
OUTLINES

✓ Background and key definitions
✓ Basic knowledge of threat and risk assessment
✓ Some examples of nuclear security violations. Lessons learned.
✓ Design Basic Threat. General approach
✓ Response to nuclear security events
Nuclear or Radiological Terrorism – no universally accepted definition

- The 2005 Nuclear Terrorism convention defines the act of nuclear terrorism as the use or threat to use nuclear material, nuclear fuel, radioactive products or waste, or any other radioactive substances with toxic, explosive, or other dangerous properties;
- The definition includes the use or threat to use any nuclear installations, nuclear explosive, or radiation devices in order to kill or injure persons, damage property, or the environment, or to compel persons, States, or international organizations to do or to refrain from doing any act.
Defining some key terms (IAEA NSS №10, 13)

**Threat** – a person or group of persons with motivation, intention and capability to commit a malicious act.

**Threat assessment** - an evaluation of the threats - based on available intelligence, law enforcement, and open source information – that describes the motivation, intention and capability of these threats.

**Design Basis Threat (DBT)** – the attributes and characteristics of potential insider and/or external adversaries, who might attempt unauthorized removal or sabotage, against which a physical protection system is designed and evaluated.

**Risk Analysis** — Process that determines likelihood that adversary (as described in DBT) will be able to bring about undesirable consequence (normally operator responsibility)

**Vulnerability** - Feature or weakness that can be exploited to cause undesirable consequence (normally assessed against the Threat or DBT).
Three types of Nuclear or Radiological Terrorism

- Detonation of nuclear bomb, either a nuclear weapon from State’s arsenal or improvised nuclear device made from stolen weapons-usable material; *
- Sabotage of a nuclear facility or transport with radioactive materials causing a large release of radioactivity;
- Use of radiological dispersal device or “dirty bomb” to spread radioactive material and create panic and disruption.

* Early was accounted in four categories (theft of nuclear weapon and use of improvised nuclear device were distinguished)
POTENTIAL NUCLEAR SECURITY THREATS

- Nuclear explosive device
  - Theft of nuclear weapon
  - Theft of nuclear fissile material for making an improvised nuclear device

- Radiological dispersal device *
  - Theft of radioactive material/source
  - Use of radioactive material out of regulatory control

- Sabotage
  - Nuclear Facility / Transport of RM to cause release of radioactivity

* For radiological weapons ("dirty bomb") see Lecture 2.3 “NFC and proliferation risks”
France Nuclear Power Plant Drones: Mysterious Illegal Flyovers Have Officials Puzzled

By Julia Glum @superjulia j.glum@betimes.com on November 03 2014 10:00

Nuclear smuggling deals 'thwarted' in Moldova
- 7 October 2015
Media caption Richard Galpin reports on the attempts by smugglers to sell nuclear material to extremist groups

Moldovan police working with the FBI are reported to have stopped four attempts by smugglers to sell nuclear material to extremists in the Middle East over the past five years.

Is ISIL a Radioactive Threat?
Posted on Nov.07, 2014 in ISIL, Radiological Terrorism by George M. Moore

Y-12 protesters allegedly enter high-security area, spray paint, splash blood
July 28, 2012 By John Huotari 3 Comments

Stuxnet: UK and US nuclear plants at risk as malware spreads outside Russia
by Alastair Stevenson , 11 Nov 2013

Al Qaeda In Pursuit Of Nuclear Weapons/Radiological Material - Analysis
Written by: Muhammad Jawad Hashmi, ScienceBlog, 24 April 2012
Inventories – facilities and materials potential targets for terrorists

> 17,000 nuclear weapons
> 3,000 tons civil and military HEU and Pu
> Around 700 research reactors (>100 with HEU)
> 100 fuel cycle facilities

> 450 operating nuclear power plants in 31 States

> 100,000 Cat I and II radioactive sources
> 1,000,000 Cat III radioactive sources
Some examples of attempts of N&R terrorism

Attack at Pelindaba Nuclear Facility (South Africa), November, 2007

- Site with 100s of kilograms 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 50 minutes inside protected perimeter
- Not 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 (DBT)
Some examples of attempts of N&R terrorism

Moldovan HEU case

- 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
- 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...
Some examples of attempts of N&R terrorism

July 2012, USA Protesters intrusion at Y-12 Facility (Oak-Ridge)

3 protesters, including an 82-year-old nun:
- penetrated to the wall of the building where 100s of tons of HEU (!) is stored

Failings of PPS:
- New intrusion detection system had been setting off huge numbers of false alarms;
- Cameras that could have assessed alarms had been broken for months;
- Guards assumed alarms were false; guards inside building assumed protesters’ pounding was construction they had not been told about.
Identify Categories of External And Internal Threats

**External threat**
- Terrorists
- Protestors
- Demonstrators
- Activists
- Extremists
- Criminals

**Internal threat**
- Insider is anyone with authorized, unescorted access who could:
  - act alone or in collusion with external threat
- May be passive or active
Threat Assessment – Country Case

State Borders

State Interior

Nuclear or radioactive materials

Target

Strategic locations

Nuclear facilities

Facilities where radioactive sources are present
Threat Assessment — Identify What Needs to be Known about Threat

- Motivation
  - Ideological
  - Personal
  - Economic

- Intention
  - Theft
  - Sabotage

- Strategies
  - Stealth
  - Deceit
  - Force

- Capabilities
  - Group size
  - Weapons
    - Specific types
  - Explosives
    - Types and quantities
  - Tools
    - Hand and power tools
  - Transportation
    - Land, air, water
  - Collusion from insider/s
  - Skills
  - Funding
  - Support structure

- Current trends and tactics
Operator and State Roles in Protection against Potential Threats

Operator Responsibility

State Role in Protection

Maximum Threat Capabilities against which Protection will be Assured

State Responsibility

Low Threat Capabilities

Some inherent protection

Planned Protection

Operator Role in Protection

Threats Evaluated in Threat Assessment

Can be equal to maximum protected threat

Maximum Threat Capabilities

Maximum Threat Capabilities against which Protection will be Assured

Design Basis Threat

Operator Responsibility

Can be equal to maximum protected threat

Some inherent protection

Planned Protection

Operator Role in Protection

Threats Evaluated in Threat Assessment

Can be equal to maximum protected threat

Some inherent protection

Planned Protection

Operator Role in Protection

Threats Evaluated in Threat Assessment

Can be equal to maximum protected threat
## Example Threat Characterization Matrix

<table>
<thead>
<tr>
<th>PROTESTORS</th>
<th>TERRORISTS</th>
<th>CRIMINALS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>MOTIVATION</strong></td>
<td><strong>Ideological, ready to kill and die</strong></td>
<td></td>
</tr>
<tr>
<td><strong>INTENTIONS</strong></td>
<td><strong>Sabotage of Plant</strong></td>
<td></td>
</tr>
<tr>
<td>Theft or Sabotage</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>CAPABILITIES</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>NUMBERS</strong></td>
<td>5 to 8 persons</td>
<td></td>
</tr>
<tr>
<td><strong>WEAPONS</strong></td>
<td>Automatic riffles</td>
<td></td>
</tr>
<tr>
<td><strong>EXPLOSIVES</strong></td>
<td>RDX up to 10 kg</td>
<td></td>
</tr>
<tr>
<td>Type &amp; amount</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>TOOLS</strong></td>
<td>Cutting Torch</td>
<td></td>
</tr>
<tr>
<td>Power or hand tools</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>TRANSPORTATION</strong></td>
<td>2-3 all-road jeeps</td>
<td></td>
</tr>
<tr>
<td>Ground, air, water</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>TECHNICAL SKILLS</strong></td>
<td>Moderate</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>FUNDING</strong></td>
<td>High</td>
<td></td>
</tr>
<tr>
<td><strong>INSIDER COLLUSION</strong></td>
<td>1 Passive, LA access</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>SUPPORT STRUCTURE</strong></td>
<td>Intern. Network</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>OTHER</strong></td>
<td>Direct attack</td>
<td></td>
</tr>
</tbody>
</table>
Facilities:
- Nuclear Power Plants
- Research Reactors
- Conversion and Enrichment facilities
- Fuel fabrication Plants
- Reprocessing Plants
- And others...

DBT: background
Design Basis Threat Life Cycle

1. Perform threat assessment
2. Define DBT
   - Competent authority
   - Government organizations
   - Shippers/carriers
   - Assumptions
3. Design PPS
   - Review by competent authority
4. Implement PPS
5. PPS assess and evaluate
   - Transport Security plan
   - Authorization to Transport
6. Maintain DBT
7. Beyond DBT
   - National organizations with PPS responsibilities
DBT: responsibility

Competent authority uses threat assessment as basis for defining DBT

- Threat assessment document
- Policy, technical and financial resources capability
- Operator competent representative
- Information analysis process

Inherent protection
Beyond the DBT
DBT
DBT can’t cover some type of threats.
State takes responsibilities on itself for certain types of threats.
For example, the war threat is fully on responsibility of the State.
Outlines legal and policy initiatives now in place
Recommends U.S. and Russian actions:
**Joint:** groups of senior officials, reporting to Presidents, to:
Develop, implement specific agenda for nuclear security, intelligence, law enforcement;
Coordinate action in nuclear terror crisis;
Share information and analysis on nuclear forensics;
**Parallel:** commit to high standards of security and accounting for all stocks, specific security practices improvements;
**With others:** strengthen the IAEA, share GICNT and CTR experience
Guards perform routine administrative duties such as escorting, administrative access control, routine patrolling, and assessment of non-critical alarms.

Response forces are responsible for delay, interruption, and/or neutralization of an adversary to prevent an undesired event, such as theft or sabotage of nuclear material.
Response Force Equipment

- Body armor and helmet
- Night vision devices
- Gas masks
- Chemical biological suits
- Miscellaneous equipment
  - Flashlights
  - Handcuffs
  - Load-bearing vest
- Armored vehicles

DBT indication of necessary equipment
Training and Proficiency Testing for Response forces

- Training on regular basis should include contingencies
- Regularly test response force proficiency in:
  - Response (time and location)
  - Required knowledge, skills, and abilities
    - Types, location, and identification of targets
    - Tactics
    - Use of force
    - Firearms

Mechanism
- Classroom
- Limited scope testing
- Force on force
What is important for effective response?

✓ **Planning**: time lines, response strategies, considering site/adversary characteristics; response force capabilities, etc.

✓ **Communication Systems**: (simple, easy to operate, efficient, low cost; approximate range is 2 to 5 Km)

✓ **Interaction with outside agencies** should be carefully planned and documented: (role and responsibilities of support agencies, communication means and procedures, on- and off-site response operations and command).

✓ **Joint training exercises** and validations.
One more about the plans

**Security Plans** – based on regulatory requirements taking into consideration *design basis threat/threat and risk assessment* and include design, evaluation, implementation, and maintenance of physical protection systems and contingency plans.

**Contingency Plans** – predefined sets of actions for *response to security events* - unauthorized acts indicative of attempted unauthorized removal or sabotage, including threats thereof, designed to effectively counter such acts.

**Emergency Plans** – predefined sets of actions for *response to safety events or other emergency events*. Measures to ensure the mitigation or minimization of the radiological consequences of sabotage as well as human errors, equipment failures, and natural disasters.
Contingency Plans

- Implemented after detection and assessment of a malicious act:
  - To locate and recover missing nuclear material
  - To mitigate or minimize effect of sabotage

- Should include the objectives, policy, and concept of operation for a systematic, coordinated, and effective response

- Documented protocols for:
  - Preventing further damage
  - Security of the facility
  - Protecting emergency equipment and personnel
Consistency of Contingency Plans

The State and License holder contingency plans should be consistent and coordinated.
Integrated Response to a Radiological Incident

Tactical Phase

Removal of the hostile threat

Operational Phase

Rescue / Establish Control of Scene:

1. Protect the Public
2. Identify and mitigate hazards:
   - Explosives, hazardous materials, electrical, etc...
3. Triage live victims
4. Increase emergency services
5. Establish site security cordons and radiological safety buffer areas

Guiding principle of radiation response and protection: Time-Distance-Shielding

Address the walking wounded

Crime Scene Phase (Radiation survey, sampling, decontamination, etc...) (NSS 22-G)
OUTCOMES

✓ Threat of nuclear and radiological terrorism is real and imminent. It demands a global coordinated response;
✓ Threat and risk assessment serve to identify motivations, intentions, and capabilities of adversaries, potential targets and consequences;
✓ Implementation and maintenance of DBT within national legal and regulatory framework are important tools for effective PPS against potential malicious acts;
✓ Coordination of response force and other national institutions is vital for neutralization of adversary and mitigation of the consequences of nuclear security incident.
Special thanks to my IAEA colleagues! Questions?

Last Slide

It’s not over...