Strengthening CBRN-Security
Creating Public Private Partnerships

Rob Duiven

November 22, 2010
‘Terrorists like Al Qaeda don’t want a seat at the table [of democracy]. They want to destroy the table and everyone sitting at it’

*R. James Woolsey, Director CIA*
‘Acquiring WMD for the defense of Muslims is a religious duty’

Osama Bin Laden, 1998
“The biggest nightmare that many of us have is that one of these terrorist member organizations within this syndicate of terror will get their hands on a weapon of mass destruction. (...) Al Qaeda is unfortunately a very committed, clever, diabolical group of terrorists who are always looking for weaknesses and openings.”

*U.S. Secretary of State Hillary Clinton, 2010*
Strengthening CBRN-Security
Creating Public Private Partnerships

National Coordinator for Counterterrorism

Current threat assessment for The Netherlands

Creating Public Private Partnerships
- CBRN-Terrorism and CBRN Security Programme
- Counterterrorism Alert System
- Security Awareness and Performance Programme

To Do List
About NCTb

- Trigger: Madrid March 11, 2004
- NCTb is appointed in April 2004 to improve Cooperation & Coordination
- Approx. 20 agencies in NL are involved in combating terrorism. They all perform their regular tasks. NCTb coordinates
- NCTb’s responsibility:
  - Analysing intelligence and other information
  - Strategy & Policy development
  - Coordinating protective security measures
- Small high-brow organization (80 fte) directly reporting to minister V&J (Security & Justice)
- Goal CBRN-programme: minimize chances of CBRN-attacks in NL
Threat assessment The Netherlands

“Chances of a CBRN attack in the Netherlands are low but conceivable”

The Netherlands are potentially vulnerable:

- Industrial infrastructure implies risk of indirect CBRN-attacks (chemical plants, transport, etc.)
- Extensive (International) Knowledge Economy
- Open borders imply a difficult to control risk

Netherlands and its foreign interests are among the priority targets of international jihadist networks
Creating Public Private Partnerships

- CBRN Programme
- Security Awareness & Performance Programme
- Counterterrorism Alert System
One percent doctrine

- Threat analysis shows the need for action, despite limited likelihood of an attack.
- In the case of CBRN-security we (have to) believe in the ‘one percent doctrine’.

“If there's a 1% chance that scientists are helping al-Qaeda build or develop a nuclear weapon, we have to treat it as a certainty in terms of our response. It's not about our analysis ... It's about our response....”

Ron Suskind, 2006
CBRN Security Programme

1. Believe in the 1% doctrine

2. Intelligence driven
   - One integrated CBRN Treath assessment
   - Create Trusted Communities
   - Share intelligence

3. Communicate about what you do and what you don’t do
Projects CBRN-terrorism in NL

1. Creating Trusted Communities
2. Sharing Intelligence: Layers of Intelligence
3. Security enhancement High Risk CBRN-objects
4. Communication about CBRN-terrorism
5. CBRN-border control / trafficking

Annex: project Homemade Explosives
Annex: projects carried out on Disaster-Management
CBRN-programme characteristics

- Choice of projects based on risk-analysis
- NCTb coordinates these projects

Acquired budgets → approx. € 100 million

- € 1,4 mil. Programme-management CBRN (2006-2010)
- € 1,5 mil. BRN-bordercontrol (2008-2010)
- € 21 mil. CBRN-respons & forensics (2008-2013)
Project Intelligence (2006-2008)

Three layers of CBRN-intelligence, so a broad variety of actors can be informed.

Intelligence → shared only with Trusted Communities

Since 2006 yearly CBRN-threat assessment by NL Intelligence and Security Services:
- Operational information
- Trends
Build trusted community on high-level (2006 - .......)
18 governmental organisations involved on highest level (DG/SG)

- General Intelligence Service
- Military Intelligence Service
- Dep. Housing / Environment
- Dep. Transport
- Dep. Agriculture
- Dep. Education
- Dep. Public Health
- Public Pros. Service
- National Police Forces
- Military Police
- Border Control Service
- Dep. Interior
- Dep. Foreign Affairs
- Labour Inspection
- Immigration Service
- Fire Brigades
- Institute Health Environment Research
- Internal Revenue Service
- NCTb is chairman
- NCTb-staff supports this group
Project Intelligence

Specific intel for CBRN clusters research facilities

- Labs
- Universities
- Research hospitals

These three main categories are divided into 19 specific clusters. If necessary, intelligence-services provide specific (trend) reports to the clusters.

Status: secret
Effect: open lines between clusters and intel-world
Project Intelligence

Dsource intel with clusters so they can take measures. Three steps:

• **Scenario’s analysis:** what occurred in history. Develop DBT’s.
• **Impact-analyses:** measures to be taken if these scenario’s occur
• **Giving detailed guidance for each cluster**

- Define the design basis threat
- Analyze impacts on measures for each clusters
- Develop detailed guidance for each cluster

Goal
- Preventing theft from objects (locations and transports)
- Anticipating attacks upon the objects themselves

Diagnosis 2006
- Endless list of CBRN-objects (laboratories, universities, hospitals, industry, nuclear facilities, etc)
- No money to take measures
Project Security Enhancement CBRN-Objects (1)

Actions taken

1. Selection of objects through a scenario based approach. Intelligence services and scientists leading. Priority objects selected

2. Designing security packages for the different types of objects (Finished)

3. Budgeting: government provides approx. 70 mln euro in period 2008-2012 to enhance security in priority objects.
Project Security Enhancement CBRN-Objects (2)

4. Now running: implementation of security packages at selected objects

5. Execution of plans finished in 2012

6. In 2008 security contract signed with chemical industry
Project CBRN-Communication (finished)

- Goal
  - Increase likelihood of early detection
  - Minimize panic during an attack
Project CBRN-Communication

• Actions taken
  • Create specific communication plan in case CBRN-terrorism occurs: messages and responsibilities are sorted out
  • Apply awareness-raising instruments:
    • Campaign to inform selected professionals (general practitioners, scientists, etc) → brochures
    • Campaign to inform media → background interviews to avoid incorrect messages
    • Campaign to inform the public → Only preparation, no active communication in view of possible side effects
Project Border-control / Detection (2006-2010)

- **Goals**
  - Overview knowledge related migration
  - Strengthen border-control agencies with CBRN-knowledge
  - Strengthen border-control agencies with technical equipment
Project Border-control / Detection

• Actions
  • Create overview knowledge related migration (done)
  • Develop CBRN awareness courses (focus on the modern threat)
  • Conduct courses for operational services
  • Design protocols for follow-up in case of detection
  • Search for quick and holistic CBRN-detection tools that can be used on airports and ports: pilot-study to develop the right concept.
International Cooperation

- European Union
  - EU CBRN Action Plan, adopted by Council Meeting on 30 November 2009

- Global Initiative to Combat Nuclear Terrorism (GICNT)
  - Plenary Meeting The Hague, June 2009

- Interpol

- OPCW
(International) Exercises

- Cobalt 2009 → ‘RN’
  - Global Initiative to Combat Nuclear Terrorism

- Bioshield Global 2010 → ‘B’
  - Interpol

- Planning: 2011: ‘C’
  - OPCW
  - .........
Related Programmes and instruments

- Counterterrorism Alert System (Alerteringssysteem Terrorismebestrijding – ATb)

- Security Awareness & Performance Programme
Counterterrorism Alert System (ATb)

- It warns the operational services and economic sectors in the event of a heightened threat.
- It enables prior measures to be taken quickly in order to minimise the risk of terrorist attacks in The Netherlands and to limit the potential impact of terrorist acts.
- Voluntary to join the system.
Counterterrorism Alert System (ATb)

ATb is an alert system for the government and economic sectors → Public Private Partnership

- Government → Information – Intelligence
  → Place in the decision making process
  → Communication (-strategy)
  → internal/external security
  → Exercises

- Private Sector
  → Commitment
  → If necessary: investments
Counterterrorism Alert System (ATb)

- Airports
- Railway
- Municipal and regional transport
- Seaports
- Tunnels and Flood Defences
- Chemical industry
- Oil industry
- Drinking water
- Natural gas
- Electricity
- Telecom
- Nuclear
- Finance
- Public events
- Hotels
Security Awareness & Performance Programme (SA&P)

- Vigilant employees are essential, in order to recognise terrorist activities and preparations thereof in time and to act adequately.

- SA&P focuses centrally on the security awareness of:
  - professionals (including management); and
  - the performance of persons
Security Awareness & Performance Programme (SA&P)

Approach:
• Identify deviant behaviour or a deviant situation in their own working environment
• This does not just help to prevent terrorism, but also to prevent other forms of crime that can affect security or harm business continuity
• continuous process
Security Awareness & Performance Programme (SA&P)

In order to promote this continuous process SA&P includes:

- Red Teaming
- Virtual Gaming
- Monitoring performance
- Embedding SA&P in education, training and exercises
- Performance Indicators / Security System Metrics

Focus on:
- ATb-sectors
- CBRNE institutions
To Do List

• Ongoing: Keep the system(s) ‘current’ → raising & maintaining (security) awareness
• Defining / Refining Performance (system performance metrics)
• Streamlining concepts, policies and regulations
• Enhancement cooperation / coordination local / regional authorities
• Challenging the system (chain of systems), national & international
• ........