Business as (un)usual
Resilience of Critical Infrastructure

Unclassified - for official use only
Outline

1. About the NCTV
2. What is Critical Infrastructure?
3. Risks to Critical infrastructures
4. Solutions and tools for CIP
5. Tool: Public private cooperation
6. Solution: From protection to resilience: CIP revisited
7. Future on CIP: working together
1. About the National Coordinator

Mission statement
- The National Coordinator for Security and Counterterrorism (NCTV) helps to keep The Netherlands safe and stable by identifying threats and strengthening the resilience and protection of vital interests.
- The purpose is to prevent or minimise societal disruption.

Main tasks
- Identifying/analysing and reducing threats and risks
- Providing surveillance and protection for persons, property, services, events and vital sectors
- Expanding and strengthening cyber security
- Resilience of locations, individuals, sectors and networks
- Effective crisis management and crisis communication
Critical Infrastructures

In the Netherlands

Critical infrastructure is the infrastructure which can cause societal disruption in case of discontinuity of service.

12 critical infrastructure sectors, 33 products and services have been defined.

In the European Union, based on the EPCIP directive

Critical infrastructure: the physical and information technology facilities, networks, services and assets that, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of citizens or the effective functioning of governments in EU countries.

2 European critical infrastructure sectors: transport and energy

UNCLASSIFIED - FOR OFFICIAL USE ONLY
# Dutch national Critical Infrastructure

<table>
<thead>
<tr>
<th>2009</th>
</tr>
</thead>
<tbody>
<tr>
<td>Telecom/ICT</td>
</tr>
<tr>
<td>Energy (Electricity, Gas, Oil)</td>
</tr>
<tr>
<td>Finance (payments and securities)</td>
</tr>
<tr>
<td>Drinking water supplies</td>
</tr>
<tr>
<td>Public administration</td>
</tr>
<tr>
<td>Law and order</td>
</tr>
<tr>
<td>Transport (airports, railways)</td>
</tr>
<tr>
<td>Dikes</td>
</tr>
<tr>
<td>Food supplies</td>
</tr>
<tr>
<td>Health</td>
</tr>
<tr>
<td>Public order and safety</td>
</tr>
<tr>
<td>Nuclear and chemical industry</td>
</tr>
</tbody>
</table>
Risks (1)
Risks (2)

- Natural
- Man-made
  - Non-malicious
Risks (3)

- Man-made – Malicious:
  - Relevant trends in terrorist threats to CIP in Western World:
  - Most incidents in jihadist conflict area’s of little relevance
    - Civil aviation clear exception
  - Top down vs bottom-up
    - Intention driven vs capability driven
  - Resilience vs target-substitution
  - Resilience: is the insider threat more relevant
Cyber: a virtual and vital society

• Cyber as a “gamechanger”
  
  • Profit-sector: chances and opportunities
  • Government: new role, enabling coalitions
  • Citizens:
    • need for (improved) checks and balances
    • privacy versus individual responsibility
  
  3 trends:
  Big data, Hyper connectivity, Disappearing borders
Solutions and tools for CIP

- National security policies include CIP

- Clear responsibility division is necessary: primary responsibility lies with the CI owner or operator

- Public private cooperation

- Knowing and doing: what is CI, what can happen and what can we do?

- Sharing information, preparing for crisis and alerting CI
The Netherlands’ national security policies

- National Security Strategy
  - including National Risk Assessment

- National Counterterrorism Strategy
  - including National Terrorism Threat Assessment

- National Cybersecurity Strategy
  - including National Cybersecurity Assessment

- All-hazards, comprehensive, multidisciplinary approach to CIP
Public private cooperation

- 80% of CI is privately owned

- PPC is fundamental to effective CIP

- Example of PPC: Alerting system Counter terrorism:
  - Commitment of critical infrastructures to implement agreed measurements in case of a certain threat level
  - Commitment of government to provide all necessary information and to alert when anything relevant occurs.
Knowing and doing: the CIP approach in the Netherlands

Assessment of Criticality
Identification of critical PROCESSES

Assessment of vulnerabilities, risks and threats
Based on standing law, regulations and assessments

Roadmaps
SMART use and/or development of instruments
### Step 1 Assessment of Criticality

#### Criteria
- **Economic impact** = costs and damage to economy
- **Physical impact** = number of deaths and severely injured
- **Societal impact** = fear, anger, disturbance

#### 2009

<table>
<thead>
<tr>
<th>Sector</th>
</tr>
</thead>
<tbody>
<tr>
<td>Telecom/ICT</td>
</tr>
<tr>
<td>Energy (Electricity, Gas, Oil)</td>
</tr>
<tr>
<td>Finance (payments and securities)</td>
</tr>
<tr>
<td>Drinking water supplies</td>
</tr>
<tr>
<td>Public administration</td>
</tr>
<tr>
<td>Law and order</td>
</tr>
<tr>
<td>Transport (airports, railways)</td>
</tr>
<tr>
<td>Dikes</td>
</tr>
<tr>
<td>Food supplies</td>
</tr>
<tr>
<td>Health</td>
</tr>
<tr>
<td>Public order and safety</td>
</tr>
<tr>
<td>Nuclear and chemical industry</td>
</tr>
</tbody>
</table>

---

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Step 2 and 3. Consequences of 2014 revision from CI Protection to CI Resilience
2015 and beyond: Need for a common framework

- Cross sectoral dependencies – also cross boundary dependencies
- Explore „new” sectors, processes, capabilities
- Develop „Capabilities catalogue” for use in crisis situations
- Working further on the European Program of CIP
QUESTIONS?