TACTICS Workshop
Countering Terrorism Threats in Cities

http://www.fp7-tactics.eu
info@fp7-tactics.eu
Oct 2\textsuperscript{nd}, 2014
Temporal Decomposition (and scope of TACTICS)

- Threat mitigation
  - TDT
  - CMT
- Attack recovery
  - CMT
  - TMT

Timeline

Information about threat

Intelligence information, or signals of a first attack

or failed attack
The same man-hour is used for actual threat mitigation, instead of resource management.
TACTICS seamlessly integrates new research results in the area of **behaviour analysis**, **characteristics of the possible urban-based targets** and **scenario awareness** into a **decision making framework** comprising of a **coherent set of tools and related processes**, supporting security forces in responding **more efficiently and effective** to a given threat in order to actually prevent the terrorist attack or to limit its consequences.
Topic SEC-2011.1.2-1 Strategies for countering a terrorist attack in an urban environment

Counter Terrorism: mitigating consequences:

• Insight in threats
• Minimise time to organise capabilities
• As (cost) effective as possible

  – Dual use of existing capabilities and resources, e.g. surveillance with camera’s of shopping malls
TACTICS system derived from realistic work process
## Atomic Surveillance Fusion Patterns

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threshold alarm</td>
<td>A value is going over a threshold</td>
<td>Burglar alarm</td>
</tr>
<tr>
<td>Profiling</td>
<td>Extrapolating a value from other values of an object, person or situation</td>
<td>Access Control</td>
</tr>
<tr>
<td>Concentric circles of protection</td>
<td>An event is happening in a compartment where it is not allowed</td>
<td>Object Security</td>
</tr>
<tr>
<td>Bag of Observations</td>
<td>Attributes of multiple objects are changing</td>
<td>Crowd Management</td>
</tr>
<tr>
<td>Scenario View</td>
<td>The relation between two objects changes</td>
<td>Lost luggage (ownership)</td>
</tr>
</tbody>
</table>
Set of Tools

1. Privacy by Design
2. Counter Bias
3. Detection of Deviant Behaviour
4. Face recognition and tracking
5. Overview of possible combinations of modus operandi
Overview of possible combinations of modus operandi

<table>
<thead>
<tr>
<th>Weapon</th>
<th>Target</th>
<th>Modus operandi</th>
<th>City type</th>
<th>Invasiveness</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vegetable picking device</td>
<td>Triangular plow</td>
<td>Tubular grabber</td>
<td>Mechanical picker</td>
<td>City type 1</td>
</tr>
<tr>
<td>Vegetable placing device</td>
<td>Rake</td>
<td>Rotating mover</td>
<td>Force from vegetable accumulation</td>
<td>City type 2</td>
</tr>
<tr>
<td>Dirt sifting device</td>
<td>Square mesh</td>
<td>Water from well</td>
<td>Slits in plow or carrier</td>
<td>City type 3</td>
</tr>
<tr>
<td>Packaging device</td>
<td></td>
<td></td>
<td></td>
<td>Invasiveness 1</td>
</tr>
<tr>
<td>Method of transportation</td>
<td>Tank system</td>
<td>Sled</td>
<td></td>
<td>Invasiveness 2</td>
</tr>
<tr>
<td>Power source</td>
<td>Hand pushed</td>
<td>Horse drawn</td>
<td>Pedal driven</td>
<td>Invasiveness 3</td>
</tr>
</tbody>
</table>
# Morphological analysis

## Urban environment

<table>
<thead>
<tr>
<th>Population density</th>
<th>Climate</th>
<th>Security awareness</th>
<th>Existing infrastructure</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

## Threat decomposition

<table>
<thead>
<tr>
<th>Threat origin</th>
<th>Capabilities</th>
<th>Target</th>
<th>Modus operandi</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

## Capability management

<table>
<thead>
<tr>
<th>Object to be observed</th>
<th>Sensor type</th>
<th>Platform</th>
<th>Reliability</th>
<th>Invasiveness</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

## Threat assessment

<table>
<thead>
<tr>
<th>Intervention phase</th>
<th>Reliability</th>
<th>Criminal phase</th>
<th>Threat dimensions</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

## Behaviour

<table>
<thead>
<tr>
<th>Threat origin</th>
<th>Types of vehicle</th>
<th>No. of vehicles</th>
<th>Usage of vehicle</th>
<th>Type of IED</th>
<th>Intent</th>
<th>Type of Explosive</th>
<th>Enhancem ent</th>
<th>Nr of device s</th>
<th>Blast Initiator</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ismaлист</td>
<td>Car</td>
<td>1</td>
<td>Vector of attack</td>
<td>VBIED</td>
<td>Suicide</td>
<td>Homemade</td>
<td>None</td>
<td>1</td>
<td>Chemical</td>
</tr>
<tr>
<td>Animal Extremist</td>
<td>Lorry</td>
<td>&gt;1</td>
<td>Escape</td>
<td>PBIED</td>
<td>Conventional</td>
<td>Civilian</td>
<td>Gas - chemical</td>
<td>2</td>
<td>Electrical</td>
</tr>
<tr>
<td>Anarchist</td>
<td>Heavy Plant</td>
<td>No intel</td>
<td>Kidnapping</td>
<td>Letter/Parcel</td>
<td>Military</td>
<td>Gas - biological</td>
<td>5</td>
<td>Radio</td>
<td></td>
</tr>
</tbody>
</table>
Privacy by Design

PbD is not the answer to all privacy risks. Even when all sorts of precautions have been taken, a smart and malign user could still use a TACTICS system in the wrong way. The sensitive and intrusive nature of a system like TACTICS requires a careful consideration and evaluation at the highest and more representative level of policy-making.

- Follow the law
- (Re)designing Privacy by Design
- Identifying privacy invading activities
- Specifying 7 + 1 principles of PbD
- Methodological approach

Invasiveness

- Surrender of autonomy / cooperation
- Level of detail of personal data
  - “By-catch” of personal data (camera versus personal tracking device)
  - More than legally allowed (espionage is more invasive than surveillance)
  - Different from communicated publicly (e.g. covert surveillance)

Solove, A taxonomy of privacy, 2006
<table>
<thead>
<tr>
<th>State of the Art</th>
<th>Beyond state of the art</th>
</tr>
</thead>
<tbody>
<tr>
<td>Defining deviant behaviour by asking security personnel what is deviant through their eyes.</td>
<td>• Defining deviant behaviour by decomposing threats into past and future modus operandi and deviant behaviour</td>
</tr>
<tr>
<td></td>
<td>• Defining specific deviant behaviour by coupling characteristics of urban environments to modus operandi.</td>
</tr>
<tr>
<td>Defining deviant behaviour without taking into account context specifics.</td>
<td>• Defining deviant behaviour, signs and hot spots for specific urban locations.</td>
</tr>
<tr>
<td>Detection and interpretation done by intelligent cameras, operators and floor security separately.</td>
<td>• Combining and interpreting deviant behaviour using all capabilities at disposal to create optimal detection circumstances.</td>
</tr>
<tr>
<td>Taking privacy into account only after the system is designed</td>
<td>• Privacy by design for counter-terrorism decision support systems</td>
</tr>
</tbody>
</table>
**TACTICS Beyond State of the Art (2/2)**

<table>
<thead>
<tr>
<th>State of the Art</th>
<th>Beyond state of the art</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adding extra personnel and physical sensors to get surveillance capabilities that are normally not present</td>
<td>• Re-using existing personnel and sensors for surveillance capabilities that are normally not present</td>
</tr>
<tr>
<td>Communication and decision about a threat or attack without taking into account risks that can influence these processes.</td>
<td>• Minimizing risks in the communication and decision making process by taking into account psychological aspects such as stereotyping and prejudices.</td>
</tr>
<tr>
<td>Each European Country has different strategies, to handle urban threats and attacks</td>
<td>• Facilitating a cross European approach at the tactical, operational and strategic level.</td>
</tr>
</tbody>
</table>
This need is actual.

- improving the preparedness of security forces,
- the capabilities at their disposal,
- and facilitating the emergence of a cross-European common approach.

(European Commission, 2011)
This approach fits actual developments.

- Re-uses existing security measures
- Investigate the use of new security capabilities like:
  - face recognition in open outdoor situations,
  - intelligent behaviour camera’s, and
  - predictive profiling
- Leading design principles:
  - privacy by design;
  - user centred design

(TACTICS consortium, 2011)
A cross European common approach is needed

There are several reasons for a common approach across Europe:

- to create support on all relevant policy levels for up to date counter terrorism tactics;
- to share information on potential attack vectors (design basis threat);
- to develop, validate and share good practices;
- to create a sizeable market for the research & development of relevant products and services against new threats, to protect new targets and to address new vulnerabilities;
TACTICS is the least invasive approach

- No duplicates of existing data collection resources;
- Additional security measures only when needed, and no longer;
- Focus on deviant behaviour means that normal behaviour can continue;
- Transparency where possible;
- Privacy by Design;
- Clear scope and goals
EU Research is valid instrument for this purpose

The objective of the [European Commission’s Research Programme’s] Security theme is to develop the technologies and knowledge for building capabilities needed to:

- ensure the security of citizens from threats such as terrorism, natural disasters and crime, while respecting fundamental rights including the protection of personal data
- ensure optimal and concerted use of available and evolving technologies to the benefit of civil European security,
- stimulate the cooperation of providers and users for civil security solutions,
- improve the competitiveness of the European security industry
- and deliver mission-oriented research results to reduce security gaps.
TACTICS

Consortium

TNO (Research)
RAND Europe (Research)
KLPD (Dutch police)
PRIO (Peace institute)
ITTI (SME)
Lero@TCD (University)
ISCA (SME)
UPV (University)
Fraunhofer (Research)
KMar (Ministry of Defense)
MPH (company)
Follow us!

info@fp7-tactics.eu

http://www.fp7-tactics.eu/
References

Selected papers and reports:

- Rest, J.H.C. van, Roelofs, M.L., Nunen, A.M. van, Deviant behaviour - Socially accepted observation of deviant behaviour for security - extended summary. TNO, 2014
- TACTICS Consortium , D2.1 Factors Overview, 2013
- TACTICS Consortium , D2.2 Requirements Specification, 2013
- TACTICS Consortium , D2.3 Scenario Specification, 2013
- TACTICS Consortium , D4.4 TDT (Non) Functional requirements, 2013
- TACTICS Consortium , D5.5 CMT Functional requirements, 2013
- TACTICS Consortium , D6.4 Information Management tool functional requirements., 2013

Selected patents:

At least three design phases

1. Proposal phase: Result is proposal (paper)

2. Project TACTICS phase: Result is validation suite (software, tools and methodologies)

3. Operational integration phase: Result is operational product(s)
Starting points

- TACTICS System (TS) is a deliverable, but not the main deliverable, it is merely a vehicle to demonstrate several concepts;

- TS is the system that is composed of the TDT, CMT and the TMT. Everything else, also other police systems, are considered “environment”.

- TS Environment includes: city infrastructure; friendly actors and information sources: “regular” security infrastructure, including police forces, private security forces; neutral actors: citizens, other public services; hostile actors: regular criminals, terrorists;

- TS temporarily connects to parts of environment during the development of a threat, and disconnects when the threat is gone;
Functional Decomposition (from proposal)
TACTICS Initiation
Setting the Scene

A city with its regular inhabitants.
A city with its regular inhabitants. Some of them are (military) police forces. There is also a city wide CCTV system in place.
Setting the Scene

A city with its regular inhabitants. Some of them are (military) police forces. There is also a city wide CCTV system in place. Friendly private security forces work in the city. In private area’s they also have some CCTV infrastructure.
A city with its regular inhabitants. Some of them are (military) police forces. There is also a city wide CCTV system in place. Friendly private security forces work in the city. In private areas they also have some CCTV infrastructure. The secret service has received intelligence and they send a message with some sparse intelligence to the police.

--- start of message ---
Source: Secret Service
Subject: Urgent Intelligence Report
Message: Al Qai’da operatives are referring to imminent drop of a large stash of firearms and explosives in the city of The Hague.
--- end of message ---
Setting the Scene

A city with its regular inhabitants. Some of them are (military) police forces. There is also a city wide CCTV system in place. Friendly private security forces work in the city. In private areas they also have some CCTV infrastructure. The secret service has received intelligence and they send a message with some sparse intelligence to the police.

Some terrorists have indeed arrived in the city. They have chosen a convention in an hotel as their target. The following slides hide this information to show only what the TACTICS system perceives.

--- start of message ---

Source: Secret Service

Subject: Urgent Intelligence Report

Message: Al Qai’da operatives are referring to imminent drop of a large stash of firearms and explosives in the city of The Hague.

--- end of message ---
A city with its regular inhabitants. Some of them are (military) police forces. There is also a city wide CCTV system in place. Friendly private security forces work in the city. In private areas they also have some CCTV infrastructure. The secret service has received intelligence and they send a message with some sparse intelligence to the police.

Some terrorists have indeed arrived in the city. They have chosen a convention in an hotel as their target. The following slides hide this information to show only what the TACTICS system perceives.

The police starts the TACTICS system.
What should we expect from this threat? What should we look for?

TACTICS Start (Threat)

Decompose (Threat)

Historic Threat Database

TACTICS System

Capability Mgt Tool

Private security firm 1
City Event Permits Database
CCTV Service Provider 1
CCTV Service Provider 2
Look for multiple terrorists; multiple targets; possible targets are large groups of people with a high symbolic profile.

TACTICS System

Threat Mgt Tool

TACTICS Start (Threat)
Highlight large groups of people

Get me a list of upcoming large scale events.

Capability Mgt Tool

FindCapabilities (Events)

Private security firm 1
City Event Permits Database
CCTV Service Provider 1
CCTV Service Provider 2

Threat Decomposition Tool

Decompose (Threat)

Historic Threat Database
TACTICS System

Threat Mgt Tool

TACTICS Start (Threat)
Highlight large groups of people
Three events are occurring, all private: Nuclear Security Summit, Philatelist Convention and Shell Shareholders Meeting
Highlight three events

This is the link to the cities permits database for private events: [URL] (username, passwd)

Threat Decomposition Tool

Capability Mgt Tool

Historic Threat Database

Private security firm 1
City Event Permits Database
CCTV Service Provider 1
CCTV Service Provider 2
Let’s focus on the private events. What modus operandi should we expect?

TACTICS Start (Threat)
Highlight large groups of people
Three events are occurring, all private: Nuclear Security Summit, Philatelist Convention and Shell Shareholders Meeting
Highlight three events

Let’s focus on the explosives. Can we detect them near the private events?

Threat Decomposition Tool
Decompose (Threat)

Historic Threat Database

Capability Mgt Tool
FindCapabilities (Explosives, Near private events)
Private security firm 1
City Event Permits Database
CCTV Service Provider 1
CCTV Service Provider 2
The locations will have been scouted before the attack. At events with important VIP’s the attackers may be loitering around the area waiting for their targets.

There is no resident sniffing capability at any of the events. Ad hoc deployment of sniffers will take 12 hours. Expected accuracy: 50%
TACTICS Validation System

As described and motivated in D3.2

Legend:
- **Green** blocks are GUI
- Black arrows are technical interfaces
- Human users are shown in dark red, including verbal communication in grey.
- Two-way communication takes up 2 rows in the tables with identical id’s: 3, 5, 15 and 16.
# TMT Modules

<table>
<thead>
<tr>
<th>Name</th>
<th>Function</th>
<th>Detail</th>
</tr>
</thead>
<tbody>
<tr>
<td>TMT</td>
<td>Give an overview of the actual situation, the threat and possible</td>
<td>Three separate GUI’s (screens)</td>
</tr>
<tr>
<td></td>
<td>prevention or response actions</td>
<td></td>
</tr>
<tr>
<td>TMT:Geo</td>
<td>Give situational awareness to TM</td>
<td></td>
</tr>
<tr>
<td>TMT:SitDB</td>
<td>Store actual situation in metadata and data</td>
<td>Contains video, tracks, detections, etc.</td>
</tr>
<tr>
<td>TMT:Fusion</td>
<td>Fuse data and information from both TACTICS and non-TACTICS capabilities</td>
<td></td>
</tr>
<tr>
<td>TMT:MACap</td>
<td>Input screen for TM to request capabilities</td>
<td>Morfological analysis view</td>
</tr>
<tr>
<td>TMT:MAThreat</td>
<td>Output screen to TM to get unbiased threat information</td>
<td>Morfological analysis view</td>
</tr>
<tr>
<td>TACTICS capabilities and Resources</td>
<td>Supply object metadata</td>
<td>Behaviour detection, person recognition, identification, tracking</td>
</tr>
<tr>
<td>Friendly capabilities and resources</td>
<td>Supply object metadata</td>
<td>Simulated</td>
</tr>
</tbody>
</table>
## TDT Modules

<table>
<thead>
<tr>
<th>Name</th>
<th>Function</th>
<th>Detail</th>
</tr>
</thead>
<tbody>
<tr>
<td>TDT</td>
<td>To support TDM to generate unbiased threat information and supply this to TM (via link to TMT)</td>
<td>Two separate GUI’s (screens)</td>
</tr>
<tr>
<td>TDT:HDB</td>
<td>Store historical incident metadata</td>
<td>Nice to have</td>
</tr>
<tr>
<td>TDT:HDBView</td>
<td>Show and search historical metadata</td>
<td>relate to configurations</td>
</tr>
<tr>
<td>TDT:MAThreat</td>
<td>Described unbiased threat information</td>
<td>Morfological analysis view; using input from HDB and TM</td>
</tr>
</tbody>
</table>
## CMT Modules

<table>
<thead>
<tr>
<th>Name</th>
<th>Function</th>
<th>Detail</th>
</tr>
</thead>
<tbody>
<tr>
<td>CMT</td>
<td>To support the CM to generate actual references to capability and resources</td>
<td>Two separate GUI's (screens);</td>
</tr>
<tr>
<td>CMT:Geo</td>
<td>Show geographic view on availability, location and QoS parameters of capabilities and resources</td>
<td></td>
</tr>
<tr>
<td>CMT:MACap</td>
<td>Show TM requests</td>
<td>Morfological analysis view</td>
</tr>
<tr>
<td>CMT:RCDB</td>
<td>Collect and store actual resource and capability metadata</td>
<td>using input from both TACTICS and friendly resources and capabilities</td>
</tr>
</tbody>
</table>
Simulated scenario's in relevant environment

TMT

TDT

HDBView: View on Historical Database

MAThreat: View on MA on Threat Decomposition

Geographic View on Threat Mgt

MACap: View on MA on Resources and Capabilities

Geographic View on Threat Mgt

Fusion Engine

CM

TDM

MACap: View on MA on Resources and Capabilities

Resource & Capabilities Metadata

HDB: Historical DB

Police cap's

Friendly cap's – not connected

Friendly cap's – connected

Friendly resources

Friendly resources – not connected

Police resources
<table>
<thead>
<tr>
<th>Id</th>
<th>Sender</th>
<th>Receiver</th>
<th>Information</th>
<th>Datatype</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>TDT:HDB</td>
<td>TDT:HDBView</td>
<td>Descriptions of historical incidents</td>
<td>texts / keywords</td>
</tr>
<tr>
<td>2</td>
<td>TDT: HDBView</td>
<td>TDT:MA Threat</td>
<td>Links between (partial) configurations and historical incidents</td>
<td>Keywords + partial configurations</td>
</tr>
<tr>
<td>3</td>
<td>TDT:MA Threat</td>
<td>TMT:MA Threat</td>
<td>Decomposed threat information</td>
<td>(partial) configurations</td>
</tr>
<tr>
<td>3</td>
<td>TMT:MA Threat</td>
<td>TDT:MA Threat</td>
<td>Suggestions to decompose</td>
<td>(partial) configurations</td>
</tr>
<tr>
<td>4</td>
<td>TMT:Geo</td>
<td>TDT:MA Threat</td>
<td>More detailed threat information</td>
<td>Free text (for logging)</td>
</tr>
<tr>
<td>5</td>
<td>TMT:MA Threat</td>
<td>TMT:MA Cap</td>
<td>Threats to find capabilities for (partial) configurations</td>
<td>(partial) configurations</td>
</tr>
<tr>
<td>5</td>
<td>TMT:MA Cap</td>
<td>TMT:MA Threat</td>
<td>Capabilities to address threats</td>
<td>(partial) configurations</td>
</tr>
<tr>
<td>6</td>
<td>TMT:Geo</td>
<td>TMT:MA Cap</td>
<td>Area selection for capabilities</td>
<td>Area</td>
</tr>
<tr>
<td>7</td>
<td>TMT:MA Cap</td>
<td>CMT:MA Cap</td>
<td>Request for capabilities, including area</td>
<td>(partial) configurations + area</td>
</tr>
<tr>
<td>8</td>
<td>CMT:MA Cap</td>
<td>CMT:Geo</td>
<td>Request for capabilities, including area</td>
<td>(partial configurations + area)</td>
</tr>
<tr>
<td>9</td>
<td>CMT:Geo</td>
<td>TMT:Geo</td>
<td>Ranked list of available capabilities and resources</td>
<td>List of capabilities + resources (URL, configuration)</td>
</tr>
<tr>
<td>Id</td>
<td>Sender</td>
<td>Receiver</td>
<td>Information</td>
<td>Datatype</td>
</tr>
<tr>
<td>----</td>
<td>--------------------------------</td>
<td>---------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>----------------------------------------------------</td>
</tr>
<tr>
<td>10</td>
<td>CMT:CapDB</td>
<td>CMT:Geo</td>
<td>Resource and capability metadata</td>
<td>Keywords + partial configurations</td>
</tr>
<tr>
<td>11</td>
<td>TMT:Fusion / Resources</td>
<td>CMT:CapDB</td>
<td>Dynamic metadata per resource / capability (availability, location)</td>
<td>ONVIF? SensorWebEnablement?</td>
</tr>
<tr>
<td>12</td>
<td>TMT:Geo</td>
<td>TMT:Fusion</td>
<td>Data request / configuration based on suggestions from CMT</td>
<td>(Capability, resources, area, parameters)</td>
</tr>
<tr>
<td>13</td>
<td>TMT:SitDB</td>
<td>TMT:Geo</td>
<td>View on actual situational awareness according to TM wishes</td>
<td>Situational awareness</td>
</tr>
<tr>
<td>14</td>
<td>TMT:Fusion</td>
<td>TMT:SitDB</td>
<td>Situation updates (tracks, recognition, detection of behaviour)</td>
<td>Object metadata</td>
</tr>
<tr>
<td>15</td>
<td>Capabilities</td>
<td>TMT:Fusion</td>
<td>Fusion</td>
<td>Object metadata</td>
</tr>
<tr>
<td>15</td>
<td>TMT:Fusion</td>
<td>Capabilities</td>
<td>Data requests / configuration updates</td>
<td>(Capability, resources, area, parameters)</td>
</tr>
<tr>
<td>16</td>
<td>Capabilities</td>
<td>Resources</td>
<td>Data requests / configuration updates</td>
<td>(Resources, area, parameters)</td>
</tr>
<tr>
<td>16</td>
<td>Resources</td>
<td>Capabilities</td>
<td>Raw data</td>
<td>Video / audio / text / …</td>
</tr>
</tbody>
</table>