In recent years the threat of terrorism in urban environments has become an important issue, emphasized by several successfully carried out terrorist attacks (New York, Madrid, London). More recent experiences reported in the global media have served to keep the perception of a terrorist threat alive, such as the failed attempt by the ‘underwear bomber’ Umar Farouk.

Most terrorist attacks or attempts within Europe have occurred at airports or other variations of public transport. Outside of Europe terrorists do not only attack public transport, but also focus on other types of locations.

When security forces are alerted to a specific terrorist threat, their main goal is to prevent or mitigate an actual attack. This process is called threat management and is supported by two sub processes: threat decomposition and capabilities management.

TACTICS introduces three roles: the Threat Manager (TM), the Threat Decomposition Manager (TDM) and the Capabilities Manager (CM). They work as a team to prevent or mitigate terrorist attacks. TACTICS aims to develop trustful and effective strategies in order to support each of these managers in responding more quickly and in a more structured, efficient way to a specific threat as well as minimizing the occurrence of false positives and negatives.
Bias is an inclination of temperament or outlook to present or hold a partial perspective and a refusal to even consider the possible merits of alternative points of view. Confirmation bias or tunnel vision (example above) is a tendency for people to favour information that confirms their preconceptions or hypotheses regardless of whether the information is true. As a result, people gather evidence and recall information from memory selectively, and interpret it in a biased way. Biases can lead to wrong decisions. Wrong decisions have financial costs and deplete available resources and diminish the fragile balance of public confidence, as in the example mentioned above.

When a specific threat becomes discernable or an actual terrorist attack occurs, security forces have to assess the situation and decide what actions are needed. The goal of this part of the work was to contribute to improving the decision support process in TACTICS by identifying different strategies to deal with common biases in decision making. The following mitigation strategies were found:

- Available information in the TACTICS tool (i.e., about threats and modi operandi) can be used to formulate sensible hypotheses about the threat. By formulating hypotheses and testing them (for example by collecting additional information) an increasingly detailed picture is built of the actual threat. This strategy helps to mitigate biases related to the limited capacity of humans to give equal attention to all signals presented to them and the irrational ways in which people collect information (e.g., to confirm their ideas, to justify previous efforts, to not have to do anything else).

- A “banner” will be implemented in the TACTICS Threat Management Tool, containing critical questions, targeted at the user, that could help him/her to avoid biases in decision making that are related to attention and information collection. The questions concern two significant decisions that are made while using the tool, i.e., identification of a location (end user marks a threat; sample critical question Which information conflicts with this threat?) and identification of a suspect (a person is marked as suspicious for camera tracking; sample critical question What makes you think this is the suspect?).

- Work processes can help to mitigate biases. For example, a team member can be given the role of devil’s advocate to avoid that somebody with a high
The Threat Management Tool (TMT) will help the Threat Manager (TM) and his/her team to achieve a Common Operational Picture (COP) and increase their situation awareness (SA) during the threat facing/neutralization tasks.

- Training should brief users on common biases (make them aware) and introduce ways to mitigate bias in the working procedures. This strategy helps to mitigate all biases mentioned above as well as biases related to the way people organise information.

- These bias mitigation elements will partly be implemented into the TACTICS tools. Measurements need to be undertaken to assess the effectiveness in specific settings.

**THREAT MANAGEMENT TOOL (TMT) DESCRIPTION**

The Threat Management Tool (TMT) will help the Threat Manager (TM) and his/her team to achieve a Common Operational Picture (COP) and increase their situation awareness (SA) during the threat facing/neutralization tasks.

The TMT will show to the TM fused and filtered information from different sources: the fusion unit module, the Threat Decomposition Tool (TDC), the Capability Management Tool (CMT) and other different information sources (including units deployed in the field) integrated in the TACTICS system. With this information the TM will be able to take more accurate decision for neutralizing the threat or mitigating the effects of the attack.

The main functionalities of the TMT will be the following:

- To show the location of the units in the field: the location of the units deployed on the field (persons and vehicles) will be shown in a GIS of the hot spot area. In addition, indoor locations will be shown depending on the building digital maps availability.

- To show information from both sensors deployed in the field (e.g. CCTV cameras) and from the deployed units portable sensors (especially video/infrared cameras). These cameras could be head-mounted, fixed, deployed and/or installed in vehicles (terrestrial, maritime and aerial).

- To show potential threats in the field: Different potential threats (e.g., suspicious vehicles, backpacks, persons and so on) can be introduced into the system in order to be reviewed by the units in the field.

- To show sensors location on the GIS: the location of the different sensors available in TACTICS (mainly cameras or units deployed on the field) will be shown to the TM in order to select the more suitable ones at each moment.

- To show fused sensor information: the TMT will show on the screen the information (Video, text, coordinates, etc.) from the different sensors integrated in TACTICS.

- To allow messaging (chat) and preformatted messages (such as key indicators to look for), providing different communication channels with the units in the field for sending orders and receiving updated information.

- To show information from the Threat Decomposition Tool (TDT) regarding potential key indicators and potential modus operandi according to the type of threat provided by the intelligence.

- To allow communication with the TDT in order to ask for updated information analysis.

- To show information from the Capability Management Tool (CMT) regarding available capabilities (including capabilities attributes). With this information the TM will be able to select/access the most suitable capability at each moment.

- To allow communication with the CMT in order to ask for updated information analysis.

- To allow 3D view of the environment (including buildings), as well as to see the world with its real elevations.

- To allow street view style view of the hot-spot.
To send and receive alarms
To stick and then send and receive objects
To allow access to heterogeneous “Open Data” access from disparate sources such as public agencies traffic control cameras, census data, terrorist attacks past events, location of banks, embassies, etc. All this information is merged and analysed using several data display formatting techniques.

Some of the above mentioned functionalities are shown in the following figures:

![Figure 1 Capabilities location and video flow playing](http://www.fp7-tactics.eu/project.html)

![Figure 2 Units location on the field](http://www.fp7-tactics.eu/project.html)

YOUR CONTACT
For more information on TACTICS, please contact: info@fp7-tactics.eu

VISIT TACTICS WEBSITE
http://www.fp7-tactics.eu/project.html