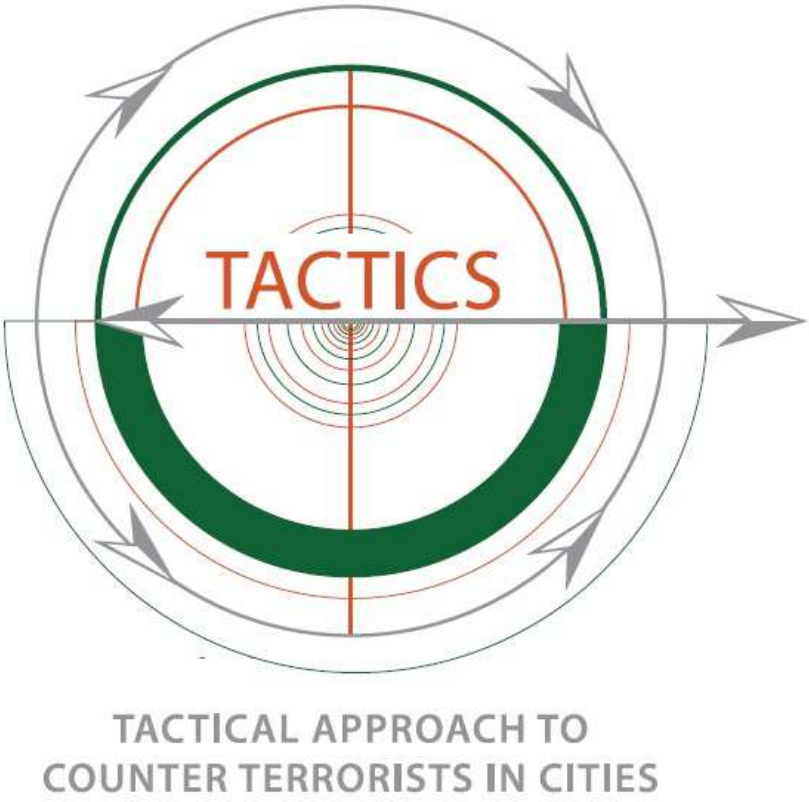
SEVENTH FRAMEWORK PROGRAMME

Collaborative project
Small or medium-scale focused research project
FP7-SEC-2011-1
Grant Agreement no. 285533



TACTICS

Tactical Approach to Counter Terrorists in Cities

Deliverable details	
Deliverable number	D3.1
Title	Conceptual Solution Description (White paper)
Author(s)	TNO
Due date	31-03-2013
Delivered date	29-03-2013 (update 11-12-2013)
Dissemination level	Public
Contact person EC	PO

Cooperative Partners	
1.	ITTI Sp. z o.o.
2.	Nederlandse Organisatie voor toegepast natuur-wetenschappelijk onderzoek TNO
3.	Peace Research Institute Oslo
4.	Rand Europe
5.	Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
6.	Universidad Politécnica de Valencia (UPVLC)
7.	Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e.V.
8.	Koninklijke Marechaussee
9.	Morpho

Table of Contents

Executive Summary

The purposes of this report D3.1 are:

- To present an integral yet generic design for a loosely coupled system of systems to be used to counter a terrorist threat in an urban environment, and;
- To guide the research during the TACTICS project phase.

This report does NOT describe the concrete validation system to be built in the TACTICS project. For the approach in the TACTICS project key aspects of the generic approach have been selected to be demonstrated in a relevant –but simulated- environment (TRL=6 [1]). Report D3.2 will focus on that particular approach.

All ideas and concepts in this report can be changed later in the project due to progressive insight or changing circumstances. Significant changes will be documented.

Problem

Over the years the threat of terrorism in European urban environments has become an important issue, first because of campaigns of organisations like IRA and ETA, and more recently by several successfully carried out terrorist attacks by Islamic terrorist groups (New York, Madrid, London) and “lone wolves” (Oslo, Boston). Also failed attempts 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.

Terrorists focus on different types of locations, many of them typically in an urban environment. Examples are the attacks in Mumbai in 2008 - where a hotel, hospital, a movie theatre, a café and other locations were hit - or the initial bombing in Oslo by Breivik. Urban environments are characterized by higher population density and vast metropolitan features as compared to their surrounding areas. Urban areas may be cities, towns or urban agglomerations. These areas are very “attractive” to terrorists since attacking them has a strong impact: high numbers of victims, high emotional and in some cases cultural value. If the Eiffel Tower would be attacked successfully, it would probably result in many victims, but it would also strike many French citizens, and Europeans, in their hearts.

When a specific threat or an actual terrorist attack occurs, security forces must answer several questions. These questions are relevant to any kind of threat, but are even more difficult to answer when dealing with urban environments:

- What are the signs of an impending attack?
- How can these signs be detected by humans or technological tools?
- How can the detected signs be fully understood?
- What actions do the signs imply?
- How to know what capabilities are at security forces’ disposal that can be used to prevent or react to an attack?
- How to decide upon the right actions in case of an actual attack?

Security forces have difficulties in answering these questions for two major reasons. First of all, most security forces in Europe do not have sufficient experience with regard to specific terrorist behaviour. Without sufficient knowledge on this behaviour it is impossible to know what the signs of an impending attack are in an urban location, how the signs can be recognised by humans or technological tools, how they can be understood and what actions the signs imply. Secondly, security forces cannot assess quickly enough what capabilities are at their disposal and what other capabilities might be necessary to deal with a specific threat or terrorist attack. They will have to be able to make this assessment quickly to decide upon the right actions, not only to prevent a terrorist attack but also to minimise the impact in terms of casualties, injuries, shock, fear and damages.

The problem of determining and detecting of terrorist behaviour can be decomposed into a set of smaller problems. We separate three aspects of this problem:

1. How can we better understand a terrorist threat? (speed, cost, quality of prediction)
2. How can we better detect precursors?
3. How can we better support decisions, while avoiding biases?

TACTICS Conceptual Solution

The TACTICS project goals are:

1. to make security forces capable of responding quicker, without being biased in decision making and to be more precise in the kind of information they request and the orders they send out by providing expert knowledge at the fingertips of the professionals of the security services at the time of an actual threat in urban environments (threat management);
2. to improve preparedness of security forces by decomposing threats into observable terrorist behaviours specific for urban environments (threat decomposition);
3. to improve the capabilities at security forces' disposal by improving their management, efficiency and their cooperation in urban environments (capability management);
4. to facilitate a cross-European approach by offering a 3-levelled strategy on the tactical, operational and strategic level.

There are two possible starting points for using a TACTICS system:

1) a message from intelligence services w.r.t. reliable information regarding a terrorist threat;
2) a more or less successful attack has happened. In this case more attacks may follow.

Both come down to reliable and validated information about a specific threat, and both will involve the proper judicial authorities to start the threat mitigation.

Both come down to reliable and validated information about a specific threat, and both will involve the proper judicial authorities to start the threat mitigation. The trustworthiness of such information is out of the TACTICS scope. The condition for stopping a TACTICS system is that management and judicial authorities believe that the specific threat on the urban environment is mitigated or they believe that there was no threat after all. The attention shifts to the investigation and crisis management phases if necessary, or to regular public order management.

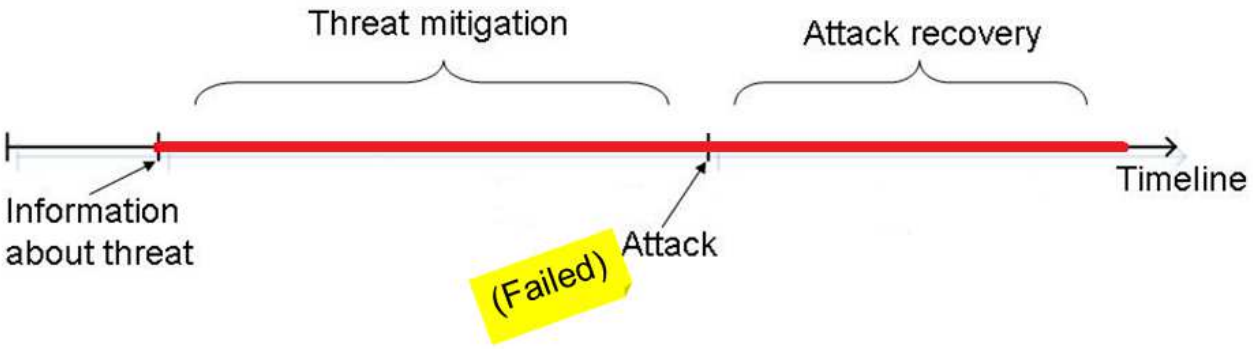


Figure 1 - The TACTICS timeline starts when information about a specific terrorist threat arrives, and ends when the threat is gone.

User centred design

TACTICS follow a user centred design by applying verified scientific and practical guidelines. This is reflected in the members of the consortium, explicit descriptions of personas and the description of a fictive storyline. A more detailed description of how TACTICS applies user centred design is described in D3.2.

Ethics and privacy

All policies and projects dealing with terrorism are particularly sensitive and challenging, not only in technical and logistical terms, but also in ethical and legal ones. The ethical starting point for the TACTICS project is to focus on the way in which specific counter-terrorism measures are designed and operated in practice, grounding their very rationale on the respect of fundamental rights. From this point of view, the assessment of the ethics and the respect of human rights should be considered a continuous process, and no blank check can be grated in advance. Therefore, specific procedures of evaluation of the potential and effective use of a counter-terrorism system should be devised and should constitute an integral part of the system itself. This is particularly important for a project like TACTICS, which purpose is to prevent or interrupt an attack, which is one of the most sensitive fields of action in counter-terrorism.

First of all, a TACTICS-like system should operate within the legal limits granted to the responsible public law enforcement agencies. As discussed in section 6 of the TACTICS Deliverable D2.1, the most prominent issue for a type of system as TACTICS is that of privacy and of data protection. In Europe, the Art. 8

European Convention of Human Rights [1] addresses privacy, as well as Art.7 of the European Union Charter of Fundamental Rights. Data protection is governed by Art. 8 of the EU Charter of Fundamental Rights and by a patchwork of legislative instruments, the most important being the data protection directive of 1995.

Privacy by Design has been dubbed by the Commission in “Data Protection by Design (and by Default)” in the proposed General Data Protection Regulation and in the proposed Directive. So, in addition to abiding to current laws, TACTICS will apply the notion of *Privacy by Design* (PbD).

Design process

Realising a TACTICS-class system requires a methodological approach, including a relevant simplification of the inherently stochastic and sometimes unpredictable life cycle phases of a TACTICS system. However, envisioning a development path with stable intermediate forms may be more crucial for the realization of a TACTICS system than the choice of a particular design method.

Conceptual Solution Description

The TACTICS approach has three pillars:

1) to support decisions with actual, relevant information and to help prevent biases;
2) to dynamically add observation capabilities to the counter terrorism force;
3) to focus on deviant behaviour as learnt from experience with terrorism.

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*. To illustrate the type of work done within these processes, 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 (Figure 11) during the development of a threat:

- The TM is responsible for making decisions based on the complete operational picture;
- The TDM is responsible for providing knowledge on terrorism, terrorist groups and modus operandi;
- The CM is responsible for providing knowledge on the current capabilities that security forces have at their disposal at the threat locations(s).

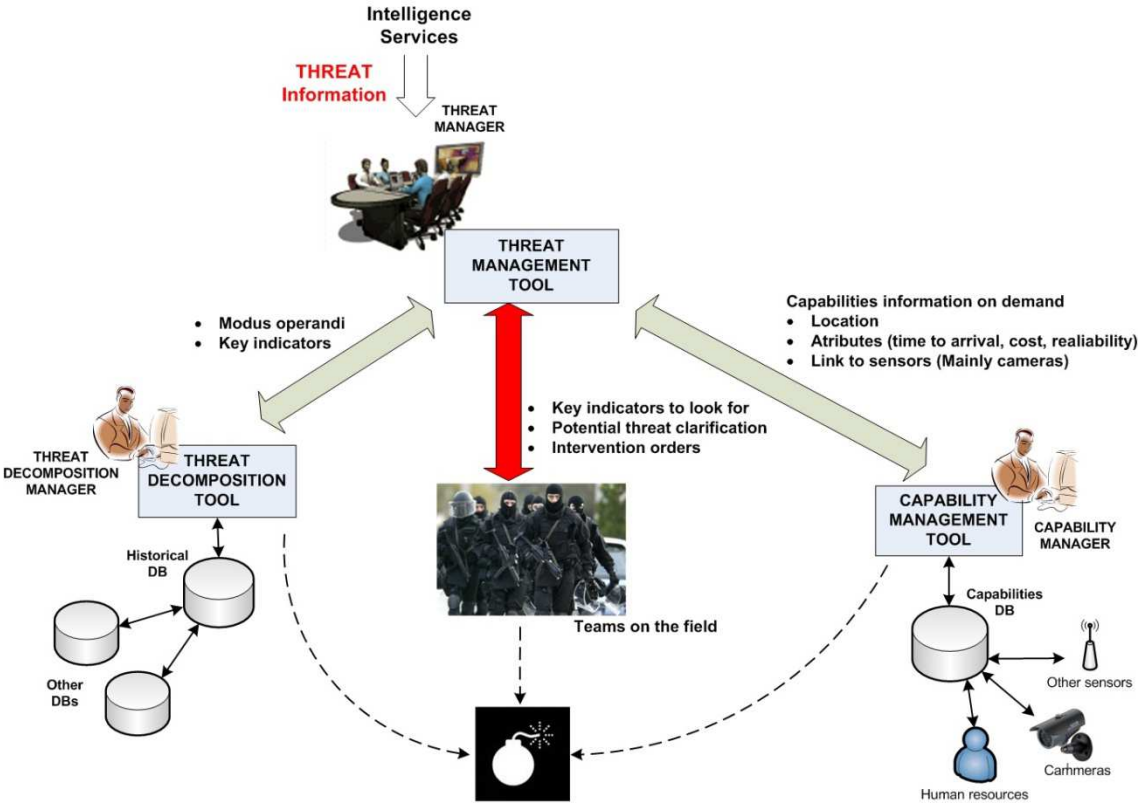


Figure 2 - TACTICS approach

Before the threat has materialized, the focus will be on understanding the threat, and on organizing the relevant capabilities to mitigate the threat. During and after the attack, the focus will shift to preventing and stopping the attack and limiting the consequences.

The purpose of the Threat Decomposition process is to improve preparedness of security forces by decomposing threats into observable terrorist behaviours specific for urban environments. As the main actor in this process, the Threat Decomposition Manager is responsible for providing knowledge on terrorism, terrorist groups and modus operandi.

The purpose of the Capability Management (CM) is to improve the knowledge on the available capabilities at security forces' disposal by improving (1) awareness about the general availability of capabilities most appropriate in a given situation, (2) access to capabilities, and (3) management of capabilities. This is done by automatically matching indicators of a potential threat to available capabilities, such as security staff, camera surveillance or detection of weapons. The matching results in a dynamic overview of most appropriate capabilities, aiming at improved detection circumstances within an urban environment, i.e. increasing the chance for prevention and timely intervention.

The purpose of the Capability Management (CM) is to improve the knowledge on the available capabilities at security forces' disposal by improving (1) awareness about the general availability of capabilities most appropriate in a given situation, (2) access to capabilities, and (3) management of capabilities. This is done by automatically matching indicators of a potential threat to available capabilities, such as security staff, camera surveillance or detection of weapons. The matching results in a dynamic overview of most appropriate capabilities, aiming at improved detection circumstances within an urban environment, i.e. increasing the chance for prevention and timely intervention.

The purpose of the Threat Management process is to make security forces capable of responding quicker, without being biased in decision making and to be more precise in the kind of information they request and the orders they send out by providing expert knowledge at the fingertips of the professionals of the security services at the time of an actual threat in urban environments.

1 Introduction

1.1 TACTICS Context

Over the years the threat of terrorism in European urban environments has become an important issue, first because of campaigns of organisations like IRA and ETA, and more recently by several successfully carried out terrorist attacks by Islamic terrorist groups (New York, Madrid, London) and “lone wolves” (Oslo, Boston). Also failed attempts 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.

Terrorists focus on different types of locations, many of them typically in an urban environment. Examples are the attacks in Mumbai in 2008 - where a hotel, hospital, a movie theatre, a café and other locations were hit - or the initial bombing in Oslo by Breivik. Urban environments are characterized by higher population density and vast metropolitan features as compared to their surrounding areas. Urban areas may be cities, towns or urban agglomerations. These areas are very “attractive” to terrorists since attacking them has a strong impact: high numbers of victims, high emotional and in some cases cultural value. If the Eiffel Tower would be attacked successfully, it would probably result in many victims, but it would also strike many French citizens, and Europeans, in their hearts.

1.2 TACTICS problem definition

The fact that it is hard to prevent a known specific threat or a terrorist from acting in urban environments can be explained in different ways. First of all, these locations are mostly crowded, which makes it harder to identify dangerous individuals. Second, some of these urban locations do not have access control, and do not have specific entrances or exits. Third, different functionalities can be found such as living, working, travelling, shopping, entertainment, education. Fourth, European cities play a big role in the practice of democracy, and could therefore be at least a symbolic target for terrorists. And last but not least, European Union citizens enjoy freedom of movement and privacy without being bothered too much by security measures making it a challenge to find a balance between security and privacy. Summarizing, urban areas are complex environments with many people with different intentions who display different kinds of behaviour and who enjoy their freedom and privacy.

When a specific threat or an actual terrorist attack occurs, security forces must answer several questions. These questions are relevant to any kind of threat, but are even more difficult to answer when dealing with urban environments:

- What are the signs of an impending attack?
- How can these signs be detected by humans or technological tools?
- How can the detected signs be fully understood?
- What actions do the signs imply?
- How to know what capabilities are at security forces’ disposal that can be used to prevent or react to an attack?
- How to decide upon the right actions in case of an actual attack?
- How to tailor their response and actions in the more effective way without disrupting core democratic activities?

Security forces have difficulties in answering these questions for two major reasons. First of all, most security forces in Europe do not have sufficient experience with regard to specific terrorist behaviour. Without sufficient knowledge on this behaviour it is impossible to know what the signs of an impending attack are in an urban location, how the signs can be recognised by humans or technological tools, how they can be understood and what actions the signs imply. Secondly, security forces cannot assess quickly enough what capabilities are at their disposal and what other capabilities might be necessary to deal with a specific threat or terrorist attack. They will have to be able to make this assessment quickly to decide upon the right actions, not only to prevent a terrorist attack but also to minimise the impact in terms of casualties, injuries, shock, fear and damages.

A low quality and/or quantity of tools and knowledge regarding these difficulties can lead to undesirable negative effects such as false positives and false negatives. A false *positive* is a result that is erroneously positive when a situation is normal. An example of a false positive is the death of Jean Charles de Menezes, an innocent Brazilian electrician, who was shot in the head 7 times by the Metropolitan Police. A *false*

negative is a result that appears negative but fails to reveal a situation. Examples of this are sadly known to all and include 9/11, as well as the Madrid and London bombings. Like false positives, false negatives have financial costs and deplete available resources and diminish the fragile balance of public confidence. The FP7 research project TACTICS is concerned with improving terrorist threat mitigation in an urban environment. TACTICS does this by researching the determination and detection of indicators (precursors) of terrorist "behaviour".

The problem of determining and detecting of terrorist behaviour can be decomposed into a set of smaller problems. We separate three aspects of this problem:

1. How can we better understand a terrorist threat? (speed, cost, quality of prediction)
2. How can we better detect precursors?
3. How can we better support decisions, while avoiding biases?

1.3 TACTICS solution direction

These are the project goals:

1. to make security forces capable of responding quicker, without being biased in decision making and to be more precise in the kind of information they request and the orders they send out by providing expert knowledge at the fingertips of the professionals of the security services at the time of an actual threat in urban environments (threat management);
2. to improve preparedness of security forces by decomposing threats into observable terrorist behaviours specific for urban environments (threat decomposition);
3. to improve the capabilities at security forces' disposal by improving their management, efficiency and their cooperation in urban environments (capability management);
4. to facilitate a cross-European approach by offering a 3-levelled strategy on the tactical, operational and strategic level.

Figure 3 illustrates how person-hours are spent during an actual terrorist threat in an urban environment pre- and post-TACTICS. During the threat's development, the focus of security forces shifts from understanding the nature of the threat, to mobilizing resources and finally to actual threat mitigation.

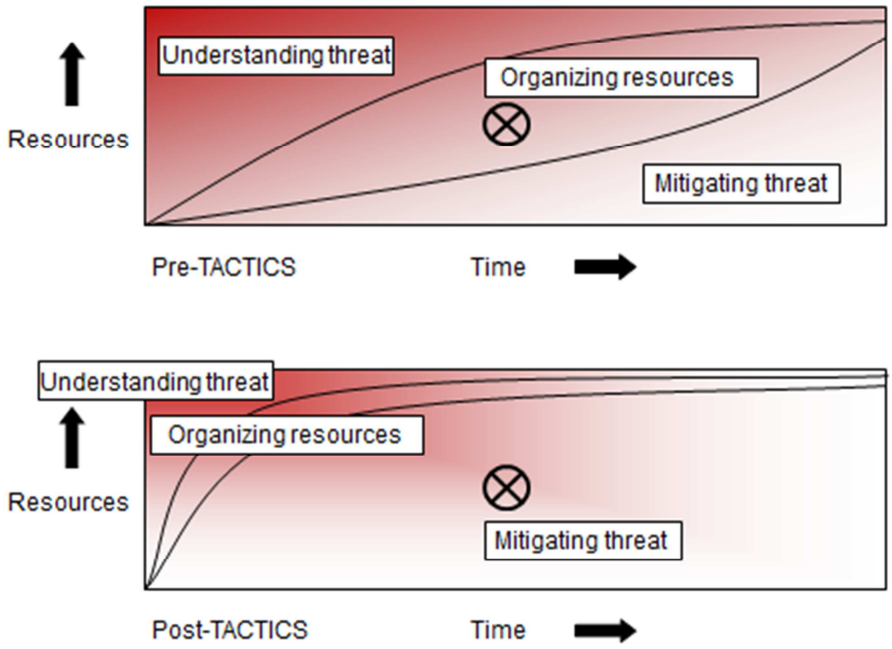


Figure 3 - A specific person-hour pre-TACTICS is still spent organizing resources. Post-TACTICS, this person-hour is spent actually mitigating the threat.

This approach is validated in the TACTICS project. The result of this validation is described in D7.1.

The project has a duration of 3 years. After this project, the knowledge built is available for future initiatives[1]. The challenges involved in mitigating a terrorist threat in an urban environment are described in D2.1-D2.4. The purposes of this report D3.1 (in order to be able to address goals 1-3) are:

(1) To present an integral yet generic approach to a terrorist threat in an urban environment;
(2) To guide the research during the TACTICS project phase.

For the approach in the TACTICS project key aspects of the generic approach have been selected to be demonstrated in a simulated environment (TRL 5 [2]). Report D3.2 will focus on that particular approach.

The mitigation of a terrorist threat is a multidimensional problem: ethical, legal, human, organisational, technological and procedural aspects must all be taken into account. The TACTICS research project therefore takes a holistic and methodological approach to manage this problem, which resembles a systems engineering[3] approach. The TACTICS approach falls –by its nature- in the class *System of Systems* engineering[4]. This class of engineering is relatively new and many concepts are still underdeveloped. Some of the inherent challenges have led to the creation of dedicated work packages in TACTICS (e.g. WP5, Capability Management). Other challenges (e.g. selection of suitable design process, meaning of privacy by design) will be addressed in this deliverable D3.1 and in D3.2.

The “TACTICS system” has a double meaning:

(1) a hypothetical class of operational systems which in some way or form resemble the TACTICS approach to mitigating terrorist threats in an urban environment. (Focus of D3.1)
(2) the concrete result of the TACTICS project; (Focus of D3.2)

In this report we use the term “TACTICS system” in the first meaning, i.e. as a hypothetical class of operational systems.

1.4 The risks of using system engineering in a research project

Using a system engineering approach for a scientific project has risks in the perception of the scientific work. For example, the software built during the project can be seen as (a preliminary version of) an operational system. Allthough this is strictly not one of the goals of the TACTICS project, TACTICS does work on dessimination and exploitation of the results. It must be noted however that the EC is not the organisation to commission the building of such a system (for a TACTICS system this would probably be a police or defense force), nor is the FP7 research framework suitable as an ICT procurement tool.

In fact, the consortium has been formed in order to achieve and validate scientific progress. In the opinion of the consortium the progress in this topic is in e.g.:
- Design methodologies (e.g. privacy by design applied to system of systems);
- Definitions of deviant behaviour and corresponding methodologies;
- Use cases for emerging technologies in the TACTICS context (face recognition and behaviour analytics);
- Work processes for counter terrorism (TM, CM and TDM);
- Prevention of biases;

The progress is not in (the development of) ICT, which can be done by regular software developers.

Another potential risk is the perception that all formulated requirements are requirements for a concrete system which is being built. Some of the requirements (D2.2 and D3.1) are intended for a hypothetical TACTICS class of systems. Other requirements (D3.2, D4.4, D5.5 and D6.4) are intended for the TACTICS Validation System. In fact, work package 7 – validation will probably generate new requirements and / or alter existing requirements for the hypothetical class of TACTICS systems.

---

[1] Goal 4 –the 3-levelled strategy- will be described in D8.1 and D8.2

[2] Technology maturity is the degree to which a technology has been proven in a realistic operational setting [38].

[3] Systems Engineering is an interdisciplinary approach and means to enable the realization of successful systems. It focuses on defining customer needs and required functionality early in the development cycle, documenting requirements, then proceeding with design synthesis and system validation while considering the complete problem [44].

[4] A system-of-systems is composed of systems which are independent, useful and used in their own right [26].

1.5 Contents of this report

This report describes the conceptual design (both as a design process, and as the result of a design process) of a TACTICS system. All ideas and concepts in this report can be changed later in the project due to progressive insight or changing circumstances. Significant changes will be documented.

Before the design of any complex system can begin, four steps must be made. In the case of a TACTICS system these are:

(1) the explanation of specialized terminology, e.g. *deviant behaviour* and *sensor fusion*; (Section 2)
(2) scoping of the problem and solution dimensions, including system maturity (Section 3)
(3) the breakdown of some relevant design paradigms into specific requirements: *user centred design* and *privacy-by-design*; (Sections 3.2-3)
(4) the selection of a suitable design process. (Section 3.4)

The main part of this report is the description of the conceptual solution description, i.e. a conceptual design: purpose and scope, functional decomposition, the level of interoperability with the environment and internal interoperability, strategies for use, key work processes and generic use cases. (Chapters 4-6)

D3.1 and D3.2 are design documents of similar systems which mainly differ in their maturity level, so they cover roughly the same topics. However, they should be readable as stand-alone documents, so they contain several very similar or even identical segments. This introduces the risk of inconsistency between D3.1 and D3.2.

2 Terminology

Shared understanding of relevant terminology is a precondition to fruitful research and design. In the domains of police, surveillance and system engineering there are several concepts which are notoriously difficult to define. The aim of this chapter is to give the definitions which are used in D3.1 and D3.2. The definitions that were used in section 1.1 are included here too.

Term	Definition
Behaviour	The reaction of a cognitive agent to a stimulus, expressed in elements of his environment.
Behaviour profiling	The extrapolation of information about a cognitive agent, based on its behaviour.
Bias	Bias is a systematic flaw in judgment, caused by a distorted image of reality. Biases are common to all humans and can pertain to attention, information processing, attribution, categorization of groups, patterns, and contextual factors such as fatigue and noise. Prevalent examples of cognitive biases are the confirmation bias, which is the tendency to seek information that corresponds with pre-existing ideas or to interpret information in such a way that it verifies pre-existing ideas [33], and stereotyping, which involves describing a person in terms of (often negative) characteristics of the group this person belongs to [9]. For an overview of cognitive biases see Baron [2].
Capability	An ability that an organization, person, or system possesses. Capabilities are typically expressed in general and high-level terms and typically require a combination of organization, people, processes, and technology (i.e. *resources*) to achieve [44]. This would be for TACTICS something like “Person Identification”, “Object Observation”, or “Area Surveillance”. In TACTICS, external (additional) cooperative capabilities are not enabled by default: based on their effectiveness against an actual threat, they may be temporarily dynamically linked to the TACTICS system, and removed again when the threat is gone.
Cognition	The ability to solve problems.
Context	The context of a surveillance system consists of the factors that influence the system and necessarily includes the environment, including people in the environment. Typical examples of surveillance context are the local culture, the level of terror threat, and the weather conditions. Additionally, world knowledge as prior probability, and known correlations between events and actions, are also a part of a surveillance system’s context.
Decision Support System	An information system that supports business or organizational decision-making activities. A TACTICS system is a decision support system for counter-terrorism purposes.
Design pattern	A design pattern is an abstraction of a design, in the sense that it is not concerned with implementation details. A *surveillance (design) pattern* is a design construct which is considered ‘good practice’ in certain application areas of surveillance. There are several surveillance patterns with similar purposes: to create situational awareness. Their structure is therefore also similar: input is raw data (video, sound, tweets, etc.), the output is a hit (alarm) or a no-hit. All require a suitable physical infrastructure and information about the context in which they are applied. Several design patterns are already prevalent in the surveillance domain –which is why we call them surveillance patterns- such as threshold alarm, behaviour profiling and concentric circles of protection. Other surveillance patterns are still emerging. Since these surveillance patterns are only concerned with structuring and analysing data, they can be applied by both machine and human. However, a human professional can shift

	seamlessly between these patterns, while machines must be explicitly designed to apply them. In both cases, the underlying information structure has its own strengths and weaknesses. Therefore, there is no perfect surveillance pattern: each pattern has to fit requirements such as efficiency, efficacy and lack of invasiveness, all of which depend on the local situation.
Deviant behaviour	(1) A reaction which does not fit to the stimulus if the intent were benign. (2) Behaviour which is not part of any of the regular processes which occur at the respective location. (3) Socially abnormal behaviour (4) Behaviour which falls outside the normal distribution of behaviour at the respective location. (5) Behaviour which is part of the modus operandi of a criminal act. (6) Behaviour which may lead to a dangerous situation. (7) Behaviour which "leaks" because the cognitive load is high when a person attempts to hide an intention. In practice, only a subset of one or more of these definitions is useful.
Environment	The environment of a system is the system's surrounding that could interact with the system. The typical environment for a surveillance system is the area under surveillance including the people under surveillance and the location(s) of the system components (including storage, data transport, monitoring room etc.).
Information Fusion	Information fusion is the merging of information from disparate sources with differing conceptual, contextual and typographical representations. There are many definitions [47] and several related concepts: **Data fusion** is the merging of data representing the same real world object. **Sensor fusion** is the combining of sensory data or data derived from sensory data from disparate sources such that the resulting information is in some sense better than would be possible when these sources were used individually. The purpose of fusion is typically to have a more accurate, more complete, or more dependable result, or refer to the result of an emerging view.
Invasiveness / intrusiveness	There is no common definition of the invasiveness of a surveillance capability. This frustrates answering questions such as "how invasive is a particular surveillance capability?", or "which is the least invasive manner of detecting a specific modus operandi?" TACTICS uses a mix of two aspects of invasiveness: the degree of autonomy which is taken from the data subject, and the level of detail of data which is observed on the data subject. Both are subjective measures. In concrete capabilities these two aspects are typically correlated: the more detailed aspect is observed, the more cooperation you need from the data subject. Technological advances allow for observing more detail at a lower level of cooperation.
Privacy	The definition of privacy –in relation to data protection- is not settled. Privacy is the ability to control and limit physical, social, psychological and informational access to the self or one's group [19]. Gutwirth writes that privacy is the safeguard of personal freedom--the safeguard of the individual's freedom to decide who she or he is, what she or he does, and who knows about it [41]. Langheinrich gives a short history of the concept of privacy by design [22], and illustrates as part of that history the origination of five specific categories of privacy that together appear to encapsulate all previous definitions: • Privacy of personal behaviour (media privacy); • Privacy of territory (territorial privacy); • Privacy of the person (bodily privacy); • Privacy of personal communications (interception privacy), and • Privacy of personal data (data or information privacy). D2.1 contains in section 6 an overview and analysis of the main legal and ethical factors involved in the TACTICS project.
Privacy by Design	The principle of 'Privacy by Design' means that privacy and data protection are

(Data protection by design)	embedded throughout the entire life cycle of technologies, from the early design stage to their deployment, use and ultimate disposal [10]. D2.1 contains in section 6 an overview and analysis of the main legal and ethical factors involved in the TACTICS project.
Privacy invading activities	Activities that potentially interfere with one's privacy [8].
Profiling	The extrapolation of information about something, based on known qualities. It leads to the identification of patterns in data of the past which can develop into probabilistic knowledge about individuals, groups of humans and non-humans in the present and in the future [40]. In the security domain, profiling means determining information about a (potential) (group of) offender(s), based on other information about the offender. Predictive profiling does this before a crime has happened. Offender profiling does this after the crime has happened, when forensic tools and methods are involved then offender profiling becomes forensic profiling. A lesser used classification is to use the type of crime as label, e.g. cyber-crime profiling. A classification which is more often used, is by type of information which is used as input (ethic or behavioural profiling) or as output (geographic profiling). TACTICS focusses on predictive behavioural profiling against terrorist attacks. Rubinstein et al give seven elements of a generally accepted framework for government data mining [39].
Resource	A physical asset, an organizational resource or a functional resource that can contribute towards fulfilling a capability. Within TACTICS this could be a type of sensor (including a human) or a database which potentially provides data and/or information to a TACTICS system, and would be combined to create *capabilities*. Examples of resources in the context of TACTICS are CCTV cameras, police officers, permit databases and private security personnel.
Scope creep	The unmanaged change of system purpose. TACTICS aims to prevent scope creep by supporting the use of the proper procedures and legislation. Re-using systems –and effectively changing their purpose(s)- generates chances for efficiency and speed. This is one of the main starting points for the TACTICS concept.
Sensor	A device which converts one energy to another, usually an electric signal, e.g. microphone, CCTV camera, pressure sensor and also the human eye. There are several closely related concepts: An active sensor sends a signal which is reflected by the subject, and/or which triggers a response from the subject, e.g. radar, sonar and lidar. An intelligent sensor applies some form of knowledge to either improve the output signal or to interpret the signal to a higher level of abstraction, e.g. a face recognition system, video content analysis and also a human. A probing sensor is a sensor with a probing mechanism with the function of bringing a stimulus to the observed subject. The response to the stimulus is measured by the sensor. Human surveillance professionals do this e.g. in Search Detect React ®[17].
Surveillance	The focused, systematic and routine attention to personal details for purpose of influence, management, protection or direction [25].
System	A construct or collection of different elements that together produce results not obtainable by the elements alone [1]. Within TACTICS the term system is a hybrid collection of machine and human components, i.e. a socio-technical system.
System of systems	The system-of-systems is composed of cooperative systems which are independent, useful and used in their own right [26]. From the point of view of managerial control, a TACTICS system-of-systems is a group of cooperative

	systems in that the central management organization does not have coercive power to run the system. The component systems must, more or less, voluntarily collaborate to fulfill the agreed upon central purposes.
Systems Engineering	Systems Engineering is an interdisciplinary approach and means to enable the realization of successful systems. It focuses on defining customer needs and required functionality early in the development cycle, documenting requirements, then proceeding with design synthesis and system validation while considering the complete problem [1].
Technology maturity	The degree to which a technology has been proven in a realistic operational setting. Not to be confused with a system's life cycle [38]. (1) Technology Readiness Level is a technology-neutral metric to assess the risk associated with technology development. (2) Integration Readiness Level is the maturity of the links between individual components (TRL); (3) System Readiness Level is a function of individual TRLs and the maturities of the links between them (IRL).
User centred design	User centred design (UCD) is a type of user interface design and a process in which the needs, wants, and limitations of end users of a product are given extensive attention at each stage of the design process. UCD can be characterized as a multi-stage problem solving process that not only requires designers to analyse and foresee how users are likely to use a product, but also to test the validity of their assumptions with regards to user behaviour in real world tests with actual users [49].

3 Design principles

TACTICS is a research project. However, it could also be seen as a tentative first design step in which a particular solution direction is investigated. From that perspective, it is wise to start with determining the scope of a TACTICS system in section 2.1. Sections 2.2 and 2.3 introduce two particularly useful concepts in system engineering: user centred design and privacy-by-design. Both define principles which lead to practical requirements, both on the design process and on the resulting system. The final section of chapter 2 discusses the design process itself.

3.1 Scoping

Scoping[5] is an essential part of both the scientific and the engineering processes. The scope depends on the authority of the team producing the architecture (based on a representation of end users, industry and RTO's in the TACTICS consortium), the objectives and concerns to be addressed (to perform research which addresses the FP7 topic text and which is guided by end user involvement) and the resources available. In the TACTICS context scoping is particularly difficult:

(1) the source and type of terrorist threats can change very quickly;
(2) the opponent is potentially highly intelligent, motivated, focused, prepared, equipped and ruthless;
(3) an urban environment is in itself highly dynamic, and all cities are unique;
(4) the organisation of counter terrorism and of required additional local capabilities differs per country, sometimes even per region or city.

The particular TACTICS approach presents additional scoping questions. If capabilities are dynamically made available and disconnected after the threat is gone (system-of-systems), then what is the scope of the TACTICS system? To address this issue, the scoping of TACTICS is done on three levels:

1. The boundaries of the TACTICS system including all cooperative systems;
2. The boundaries of the TACTICS system including all connected capabilities from cooperative other systems;
3. The boundaries of the TACTICS system without any connected capabilities from cooperative other systems (i.e. the core TACTICS system);
4. The scope of the internal components of a TACTICS system (internal decomposition).

Applying and respecting the proper (legal) procedures should prevent scope creep, while enabling the repurposing of friendly capabilities.

Levels 1, 2 and 3 are illustrated in Figure 4. By explicitly describing these three levels, the scope of a TACTICS system should remain manageable.

In addition to the scoping question, this figure also introduces the notion of *attitude* of other systems and of the environment towards security in general, or towards a TACTICS system in particular. In the context of TACTICS, the terrorist (group) is a hostile system, but the presence of an organized crime unit might also influence the counter terrorist response. Non-cooperative systems are systems which are not hostile but also not particularly cooperative towards the cause of preventing or mitigating a terrorist attack. These could be parties who demand some form of payment which is out of proportion to their services, or a group of citizens with a deep distrust against the security forces. A neutral system could be a party that wishes to ignore the threat for one reason or another. Many ordinary urban citizens could be considered "neutral" for all practical purposes. With regard to the attitude of an environment, one could say that a city who is security minded is a friendlier environment than a city with a lot of organized crime, or even a city which is de facto an urban warzone. This could e.g. influence the manner in which the wisdom of the crowd is used to mitigate a terrorist attack in a particular city: an environment like Londonderry, Kabul or Baghdad is in that sense certainly different from Madrid, Oslo or London.

[5] Scoping in system engineering context is determining the boundaries of a system. The purpose of scoping is to help manage unwanted changes in the requirements or specifications of a system, i.e. scope creep.

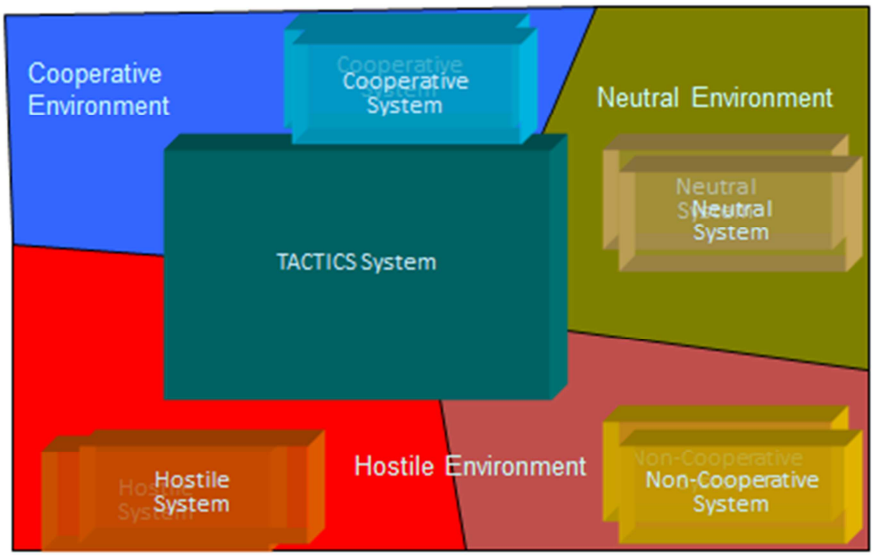


Figure 4 - Scoping a system-of-systems in a mixed-attitude environment.

Another dimension is that a TACTICS system is a hybrid composition of man (human as sensor, human as functionary/ internal user) and machine components. We identify one end user: the commander of the counter terrorist operation as the threat manager: decision maker (TMDM). All other users are “internal users”, i.e. can be considered part of the system. Three internal roles have been identified which are part of the TACTICS system, and one additional role as part of a cooperative system. This is illustrated in Figure 5.

- End user: commander of the counter-terrorist operation;
- Internal user: threat manager (analyst-level);
- Internal user: threat decomposition manager;
- Internal user: capability manager;
- Cooperative system: this could be a human as a sensor, e.g. a private security officer, but could also be a technical system.

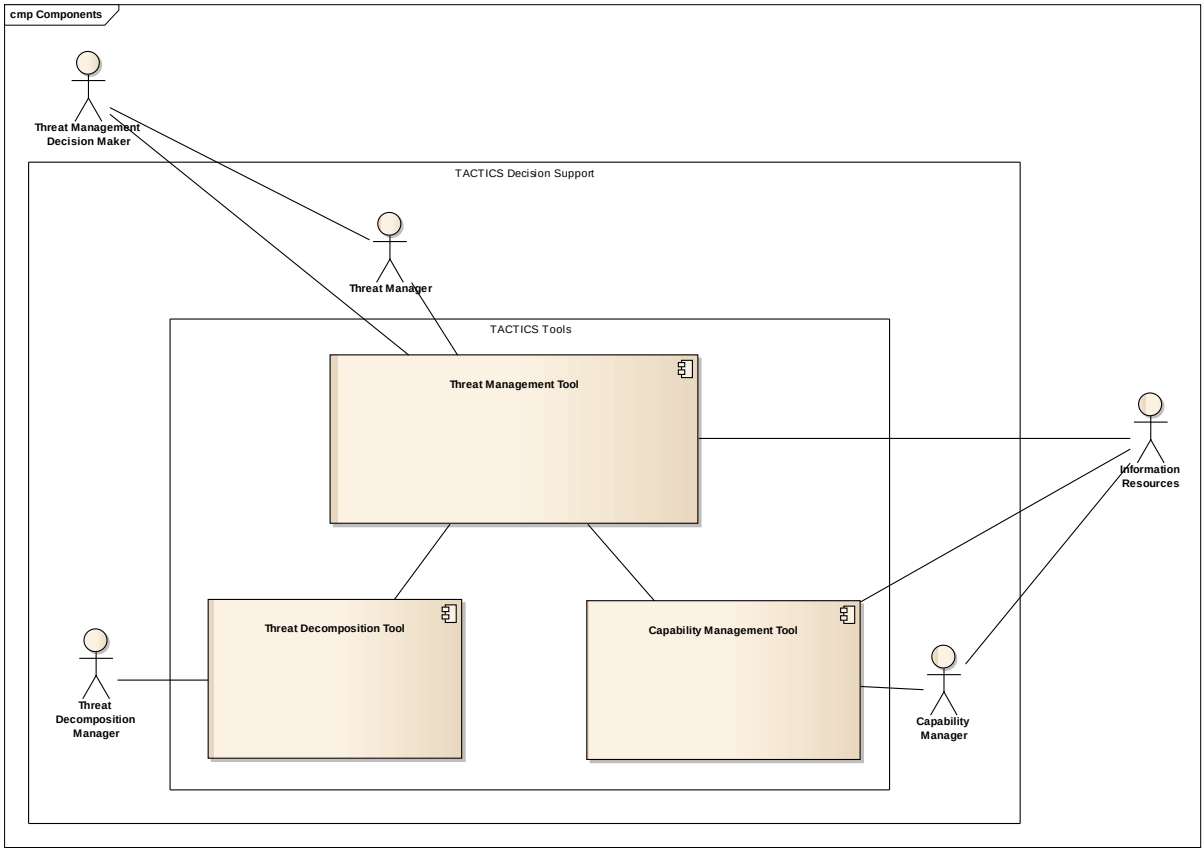


Figure 5 - TACTICS is a hybrid composition of human and machine components.

TACTICS as a project is focused on the operational level. For the sake of simplification, the role of the commander of the counter-terrorist operation is merged with the threat manager (analyst level).

Scoping must be done from different perspectives or views, of which the physical/technical and procedural view are most relevant for TACTICS[6]. TACTICS focusses on an urban environment as the target of a threat, but information coming from other environments (such as airports) is relevant to address the threat. TACTICS is not concerned with intelligence gathering, or with investigation or crisis management after the (failed) attack. We do address the concerns and needs of these other processes. For example, the intelligence process is typically separated from threat mitigation for legal and security purposes. The initial intelligence message that initiates a TACTICS-run is therefore typically very brief. Another example is the investigation process. A TACTICS system should collect and store data such that it is also useful for the investigation of a (failed) attack. This is an important reason why CCTV has such a prominent place in TACTICS, as in many security systems.

Scoping of TACTICS	In scope	Out of scope
Physical / technical	Cities	Airport, Sea border, Land border, Cyber
Procedural	Threat mitigation (including prevention and intervention)	Intelligence gathering, Crisis Management, Investigation

There are two possible starting points for using a TACTICS system:

1) a message from intelligence services w.r.t. reliable information regarding a terrorist threat;
2) a more or less successful attack has happened. In this case more attacks may follow.

Both come down to reliable and validated information about a specific threat, and both will involve the proper judicial authorities to start the threat mitigation. The trustworthiness of such information is out of the TACTICS scope.

The condition for stopping a TACTICS system is that management and judicial authorities believe that the specific threat on the urban environment is mitigated or they believe that there was no threat after all. This is a sensitive part, because it is very difficult to know that a threat has been mitigated, especially when no suspect has been caught, or when he is not properly interrogated and investigated yet.

After the TACTICS system has stopped, the attention shifts to the investigation and crisis management phases if necessary, or to regular public order management.

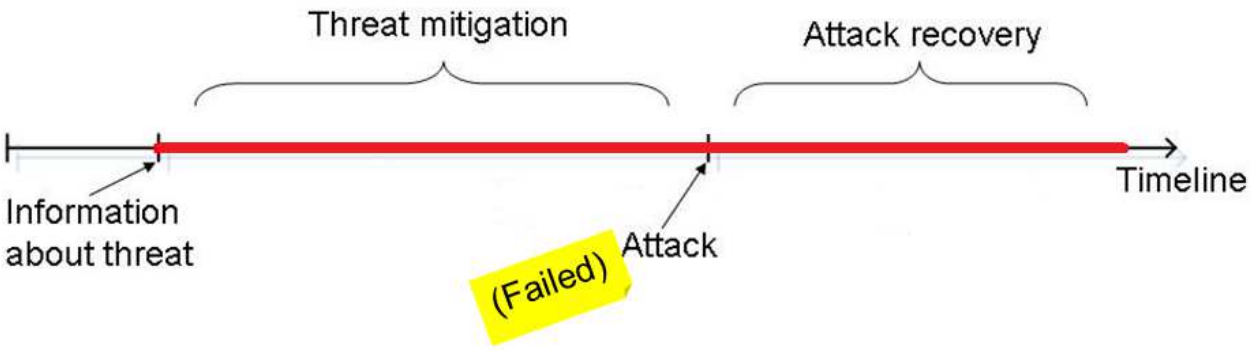


Figure 6 - The TACTICS timeline starts when information about a specific terrorist threat arrives, and ends when the threat is gone.

[6] There is no consensus on system views, and which are the elements per view. Several system engineering philosophies have proposed more or less coherent sets of system views. Estefan gives a survey of existing methodologies and views [13].

3.2 User Centred Design

Once a solution direction has been proposed, user centred design can be applied to make sure that designers and researches remain focussed on the people that actually have to use the solution. User centred design is detailed by Gulliksen [18] with twelve specific principles. All of these principles should be taken into account in the design phase of a TACTICS-class operational system. Report D3.2 describes how the TACTICS project and consortium addresses these requirements.

In this section we have recommendations for two specific principles for the design phase of an operational TACTICS system: user focus and active user involvement. Section 2.4 will discuss principles from UCD which apply to the design process.

One requirement is user focus: the goals of the activity, the work domain or context of use, the users' goals, tasks and needs should early guide the development. This can be done by making descriptions of most relevant end users, i.e. personas, and to put these personas central during design decisions. In the case of a TACTICS system it is recommended to do this for at least these end users:

- Threat manager;
- Capability manager;
- Threat decomposition manager;
- Terrorist;
- Police officer on the street;
- Private security agent;
- Socially deviant citizen;
- Socially normal citizen.

Annex A contains an initial description for each of these personas.

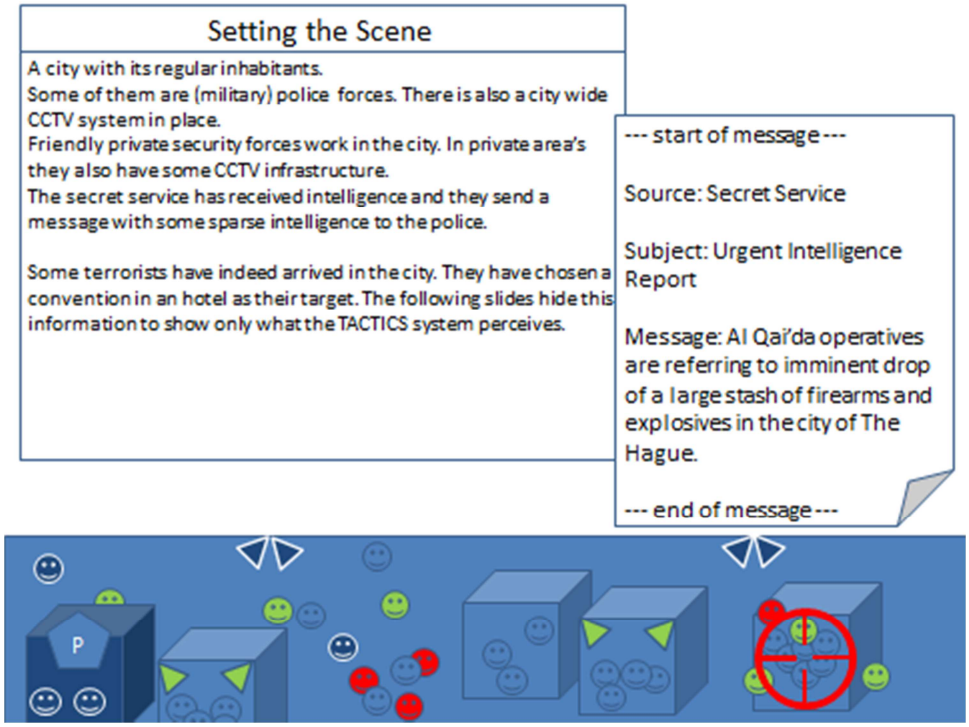


Figure 7 - Some actors in the TACTICS context. Blue faces are police officers, green faces a friendly forces, e.g. private security forces, blue faces are neutral citizens and red faces are terrorists. Triangles are sensors, e.g. CCTV. The boxes are buildings, with a police station to the far left. This picture makes no distinction between socially normal and socially deviant citizens.

Another requirement is active user involvement – representative users should actively participate, early and continuously throughout the entire development process and throughout the system lifecycle. This principle can be addressed with role playing games early in the design phase, especially with representatives of the capabilities that are dynamically made available, but are not available under normal circumstances. A user workshop with end users was done to play a serious role playing game in the TACTICS context. To help end users to imagine the setting, the start of a storyline was shown. This storyline is included in Annex B.

3.3 Ethics and Privacy by Design

All policies and projects dealing with terrorism are particularly sensitive and challenging, not only in technical and logistical terms, but also in ethical and legal ones. The ethical starting point for the TACTICS project is to focus on the way in which specific counter-terrorism measures are designed and operated in practice, grounding their very rationale on the respect of fundamental rights. From this point of view, the assessment of the ethics and the respect of human rights should be considered a continuous process, and no blank check can be grated in advance. Therefore, specific procedures of evaluation of the potential and effective use of a counter-terrorism system should be devised and should constitute an integral part of the system itself. This is particularly important for a project like TACTICS, which purpose is to prevent or interrupt an attack, which is one of the most sensitive fields of action in counter-terrorism.

First of all, a TACTICS-like system should operate within the legal limits granted to the responsible public law enforcement agencies. As discussed in section 6 of the TACTICS Deliverable D2.1, the most prominent issue for a type of system as TACTICS is that of privacy and of data protection. In Europe, the Art. 8 European Convention of Human Rights [1] addresses privacy, as well as Art.7 of the European Union Charter of Fundamental Rights. Data protection is governed by Art. 8 of the EU Charter of Fundamental Rights and by a patchwork of legislative instruments, the most important being the data protection directive of 1995. Personal data protection can be seen as a subset of privacy (e.g. excluding Solove's[7] "Invasions" [8]). An EU directive must be integrated in the national legislative body of all EU Member States. Hence, the specific implementation of a TACTICS system depends on national laws [11]. There are a new Regulation and also a new Directive being proposed by the Commission in 2012. Once adopted, especially the new Directive, focusing on the protection of personal data in the justice and home affairs domains, will become particularly relevant for the development and deployment of TACTICS. Nevertheless, as the new Directive will have to be implemented by national laws, the national legal framework will remain relevant, and it is possible to foresee differences in the implementation in each national setting.

Privacy by Design has been dubbed by the Commission in "Data Protection by Design (and by Default)" in the proposed General Data Protection Regulation and in the proposed Directive. However, there is no specific definition of what is "Data protection by design" apart from a sort of 'consistency' check that all the different data protection requirements are taken into consideration. Art. 19 of the new directive:

Article 19

> *Data protection by design and by default*
>
> *1. Member States shall provide that, having regard to the state of the art and the cost of implementation, the controller shall implement appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of provisions adopted pursuant to this Directive and ensure the protection of the rights of the data subject.*
>
> *2. The controller shall implement mechanisms for ensuring that, by default, only those personal data which are necessary for the purposes of the processing are processed.*

Art. 19[2] is more interesting, as it links data protection by default to data minimization (without explicitly mentioning data minimization).

So, in addition to abiding to current laws, TACTICS will apply the notion of *Privacy by Design* (PbD). As illustrated above, PbD is not very formally or strictly defined. Van Rest et al [36] review several existing definitions, and have proposed a more specific definition which links the EC communications with the foundational principles of PbD [5] and which also takes the application domain into account:

> *The principle of 'Privacy by Design' envisions that privacy and data protective measures are operative throughout the entire life cycle of technologies: from the early design stage to their deployment, use and ultimate disposal. This is done by applying a design process that covers all life cycle stages and by applying privacy and data protection design patterns which are well understood and are the known best-practice for the particular purpose they are used for, and domain they are used in. The resulting design documents and systems should limit all the privacy invading activities to the minimum according to the foundational principles of privacy by design.*

[7] Solove mostly uses the US case-law and US framing of privacy to build his theory of privacy. The general idea of grouping different kinds of privacy invasions might be applicable also to the European context, and useful to methodologically analyse a systems privacy impact.

3.3.1 PbD: Entire life cycle of technologies

TACTICS as a project covers only a tentative exploration of a particular solution direction, i.e. a very early design phase. The actual operational realization of a TACTICS system requires the involvement of many construction partners, and may have to be repeated for each (EU-) state. So, researchers cannot guarantee that a TACTICS system is always used properly. It is a shared responsibility with designers and end users to address the risks of data leaks, dual use, drifting and scope creep in the use phase, and the risk of data leaks in the system end-of-life phase. These risks can only be mitigated if the respective design processes actually cover all life cycle stages, including run-time and end-of-life. Users of a TACTICS system have to be made aware that they cannot put the complete responsibility of a tool like TACTICS on its researchers or designers. Users carry responsibility for specifying, procuring and using a TACTICS system properly, researchers and designers carry responsibility for creating the proper methodologies and building blocks to make this possible.

3.3.2 Prevention of Dual Use

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

More control during the use-phase of a TACTICS system is recommended. Specific examples for recommendations can be taken from efforts to control other dual use technologies: e.g. biological, nuclear or chemical technologies. Export control is one of those measures: to prevent technology to fall in the hands of those that might use it in an inappropriate manner, such has been done with Syria [7]. Education and training are another: to show end-users and internal users the consequences of miss-use and to show how to prevent, detect and signal it. Transparency about actual usage is a third measure: warrants should be obtained before certain actions can be taken and audits should be performed of the collection, processing, dissemination and destruction of personal data.

3.3.3 Identification of Relevant Privacy Invading Activities

In order to maintain and restore a level of security during a specific terrorist threat in an urban environment a TACTICS system employs privacy invading activities – as defined by Solove [8], such as:

- adding invasive (in the literal definition of Solove) observation capabilities, including stimulating persons of interest (probing) to gather their responses;
- collecting information through surveillance - including using third party capabilities;
- and processing this collected information for threat mitigation.

This is illustrated inFigure 8. When needed, the acquired data and information is made available for additional processing in a judicial investigation after a threat has been mitigated.

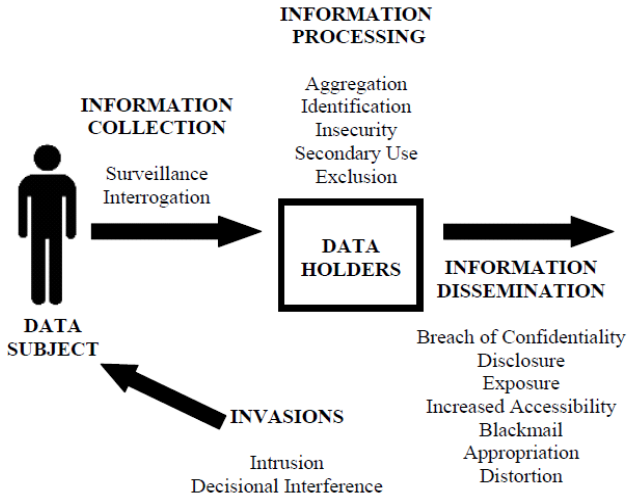


Figure 8 - Sixteen potential privacy invasions of a generic system, grouped by invasion type, as described by Solove.

Solove's typology is a useful abstraction of the relevant interaction between a data subject and a surveillance system. However, in the case of TACTICS, we need a view which also shows the composition of different cooperative systems, which is illustrated in Figure 9.

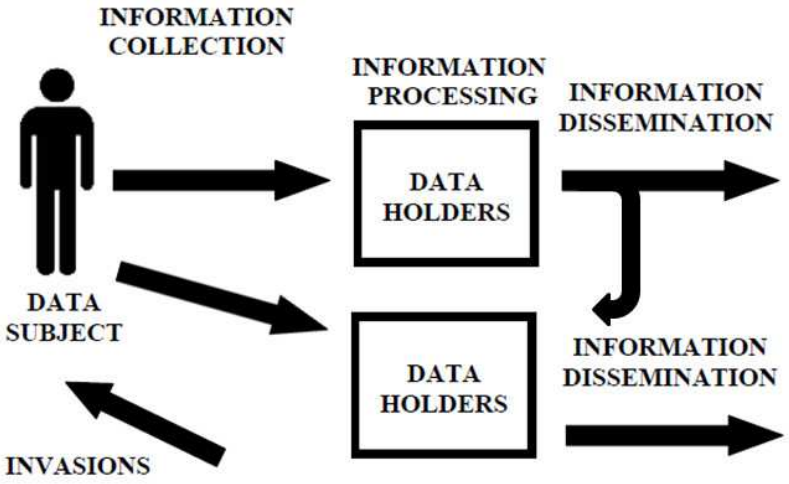


Figure 9 - Solove's typology extended for a system-of-systems context. The counter terrorism force would be the lower data holder, receiving data from cooperative data holders.

For each of these risks we recommend certain checks-and-balances to mitigate the risk of unwanted privacy breaches according to the principles of privacy-by-design.

Inparticular, several proposed solutions in this report will result in an increase in stored personal data (e.g. increasing the number of camera's, changing the types of camera's, using face recognition or behaviour analytics). This is a data protection issue which must be properly addressed. In addition, the effect of a data breach can increase when a tracking and finding surveillance system is in place. Depending on the implementation of the system, if data is stored in the form of tracks or (cut-out) clustered images of people, then it is much more easy to do harm with the data. Finally, some solutions (not part of the TACTICS Validation system) propose to send images out to professionals on the floor on mobile ICT devices. This carries additional data protection risks and also security risks.

3.3.4 Foundational principles of PbD

The seven foundational principles of Privacy-by-Design [5] should be applied during the design phase of a TACTICS system[8]. Between brackets the privacy invading activities of Solove are indicated which should be mitigated by the specific implementation of these principles (I=Invasions, C=Collection, P=Processing and D=Dissemination). We recommend addressing them as follows:

- **Proactive not Reactive; Preventative not Remedial**: Organize an independent Privacy Impact Assessment by a recommended organization as soon as the first integral outline of a design is available [45]. And carry on regular Privacy Impact Assessments (PIAs, or Data Protection Impact Assessment - DPIAs, as dubbed by the Commission), which are not mentioned in the proposed Directive but are one of the major innovations advanced by the General Data Protection Regulation. (D)PIAs are also increasingly used to assess law enforcement systems, including counter-terrorism ones. The possibility to use DPIA on a regular basis, and every time that TACTICS is activated (which will occur only in major occasions), would help ensure that privacy and data protection requirements remain center-stage and assessed from the design and during the operative life of the TACTICS system. (ICPD)
- **Privacy as the Default**: Security forces using a TACTICS system have by default no access to additional capabilities. Only when a specific terrorist threat is present, these additional capabilities will be unlocked. And after the threat is mitigated, access to these additional capabilities will be revoked again. In addition, people that behave normally during the threat, will by default not be inspected as elaborate as people that show deviant behaviour. (I) Information collected by the counter terrorism forces directly, or through the use of cooperative data holders should not be disseminated further by the counter terrorism forces. This assumes that the investigation organisation is part of the counter terrorism forces.
- **Privacy Embedded into Design**: the focus on behaviour throughout TACTICS is a way to incorporate the proportionality principle: you might draw attention by what you do, not by aspects that an individual does not have control over, e.g. skin colour, ethnicity or sexual orientation. (I) A second action could be the appointment of a TACTICS-system Data Protection Officer (following both the text of the proposed Directive and the growing practice of many LEAs). (ICPD) A third action is the inclusion of encrypted

[8] D3.2 will discuss the specific measures taken in the TACTICS project.

hashes when combining resources from other entities in order to avoid getting “too much” data, but still being able to find relevant data on threat indicators (PD).

- **Full Functionality – Positive-Sum, not Zero-Sum**: The ambition of TACTICS is indeed that security and privacy can be designed in the same system. The dynamic nature of giving and revoking access to capabilities depending on the presence of a threat, the default setting of no-access, and the ability to zoom in on people that show deviant behaviour, while leaving others alone, create a positive sum scenario.(ICPD)
- **End-to-End Security – Lifecycle Protection**: Part of the impact after TACTICS will be that security forces have a better information position than pre-TACTICS. With regard to the data lifecycle we recommend using design processes which actually cover the complete life cycle of a TACTICS system in the next section. With regard to the data of additional capabilities, in the case of actual crimes, any relevant data will have to be passed to the Investigation process. Data which would also have been acquired for non-counter terrorism purposes will follow the normal data lifecycle. (ICPD)
- **Visibility / Transparency**: For security reasons involved in counter terrorism not all data and information can be made public. However, transparency can be obtained about the use of the system with mandatory warrants and audits. (ICPD)
- **Respect for Users**: In the context of a TACTICS system, respect for users should be interpreted as respect for urban citizens. Ultimately, this is about the balance of power between the observant, and the data subject. This could be implemented by requiring one-time, temporary credentials to access a TACTICS system, which will have to be renewed after a short period, e.g. one week. If the end of the week approaches, and no new credentials have been submitted, then a notification to the proper legal authorities and/or data protection authorities will be made. In addition, TACTICS will recommend to use the least invasive surveillance capability as possible. The next section describes how the TACTICS validation system will interpret invasiveness. (ICPD)

In addition to these seven principles, an eight principle might be valuable: data minimization. Data minimization is probably one of the key elements of a PbD approach that aims at being something more than a checklist or a laundering process for surveillance measures. However, data minimization can sound at odds with the very premises and ambitions of a ‘system-of-systems’ such as TACTICS, which aims at digesting a very wide range and number of data. A possible PbD solution is to further work on scoping so to make it becoming a sort of variable geometry scaling (not everything is connected at the same time since minute zero, but different configurations of connection and of storing are available). Also, further attention should be paid to the quality of the processing so that better information can be extrapolated from less data (a sort of reversal of the lures of Big Data). (CPD)

3.3.1 Invasiveness / intrusiveness

There is no specific common definition of invasiveness in relation to surveillance capabilities. In TACTICS we define invasiveness as a combination of two factors: the degree of autonomy which is taken from the data subject, and the level of detail of data which is observed on the data subject. Together these two factors create a two dimensional scale of invasiveness which is described in Table 1.

Table 1- Levels of invasiveness

Levels of invasiveness		Reduction of autonomy of subject						
		Subject does not have to cooperate			Subject cooperates			
		None	Informed	In view	Carrying	Request behaviour	Limit behaviour	At disposal
Level of detail of personal data	None	No surveillance (0)	Fake surveillance measures					
	Location and appearance	Hidden surveillance without consent	Hidden CCTV camera with informed consent (1)	Human surveillant, CCTV camera		Face recognition under controlled circumstances	Strong probing actions (5)	Interview
	Identity and location		Hidden CCTV camera with stand off face recognition; Mobile phone	CCTV camera with stand off face recognition (2)	Mobile phone; Active RFID; GPS transmitter (3)			
	Reaction to stimulus			Any visible sensor is also a stimulus		Moderate probing actions (4)		Interrogation
	Under clothing					Mmwave radar		Frisking (6)
	Internal objects					X-Ray		Internal investigation (7)
	Physiological factors				Heart rate and temperature monitor	Camera met hartrate monitor or with infrared temperature monitor		Lie detection machine (8)

In certain circumstances tt is more practical to use a one-dimensional scale, and / or to reduce the number of levels. Table 2 describes a nine-, or a four point scale of invasiveness.

Table 2 - Four- and nine level scales of invasiveness

Invasiveness (4 point)		Invasiveness (9 point)		Description
A	None	0	None	There is no surveillance
B	Slight	1	Knowing	The subject knows that he is being monitored, but does not see, have to carry or do anything special (e.g. you assume that a certain fraction of the subjects carries mobile phones which you can monitor);
		2	Seeing	The subject sees the devices monitoring him around him, but he does not have to carry something or act in a special way;
C	Moderate	3	Carrying	The subject carries a device which is being monitored. The device does not require any special acts in order to be monitored, e.g. a GPS tracking device;
		4	Acting	Acting (i.e. cooperation): the subject regularly has to act in a certain way in order to be monitored, e.g. have biometrics taken in a controlled environment, or offer an RFID card to a reader;
		5	Possibly interrupting	The monitoring agent (device, etc.) has the option to interrupt when he sees fit, but this is not certain, e.g. a police officer standing next to a people flow;
D	Strong	6	Interrupting	The subject knows he will actually be interrupted in his normal behaviour in order to respond to a probe or an information-request, e.g. a reception desk at a secured object;
		7	Bodily	The subject has to give physical access to (a part of) his body, e.g. a pat down at an airport.
		8	Full transparancy	The subject hands over control over his body and allows monitoring of his internal physiological factors

Depending on the chosen definition of deviant behavior, it is possible to use these scales to indicate the level of invasiveness which is required to detect it in certain circumstances. The level of invasiveness that is required that is required for a specific surveillance capability (e.g. detecting deviant behaviour) depends on the chosen definition of deviant behaviour, the context (e.g. weather) and environment (e.g. indoor or outdoor), available budget and other circumstances.

3.3.2 Data security

TACTICS as a research project does not focus especially on data security because, as the end users are typically defence and police organisations, they will already have appropriate data security policies and measurements in place. The TACTICS Validation system will apply appropriate data security measurements.

3.4 Design Processes

Realising a TACTICS-class system requires a methodological approach, including a relevant simplification of the inherently stochastic and sometimes unpredictable life cycle phases of a TACTICS system. The concepts of UCD and PbD both add specific principles, which apply to the design process itself. UCD requires an evolutionary approach, simple design representations, yet a holistic design, explicit and conscious design activities, yet also process customization. PbD requires the design process to cover not only the design phases of a system's life cycle, but to start before a particular solution direction is investigated, and to continue after the design phase into the use phase and the end-of-life phase of the system.

Traditional linear models such as the V-Model are not adequate for these design processes. Take, for example, the Waterfall model: a simple and widely taught process model for designing systems. It consists of

the phases Specification, Implementation, Integration, Test and Maintenance. However, the definition for PbD from the Commission itself references other phases in the life cycle of systems: the deployment, the use and the disposal phases. This disqualifies the Waterfall model for PbD because it does not acknowledge the importance of how the system is actually used, or of data disposal at the end of the life cycle of a system. Another issue with the Waterfall model is that it assumes that all stakeholders know what the problem is and on top of that, wastes no time deliberating different solution directions. The first phase of the Waterfall model is directly the requirements phase. The motivation for a particular solution direction stays implicit, and the Waterfall model is therefore not transparent. This is a risk for keeping and gaining trust.

Another issue is that of repurposing a system, which may seem –from the point of view of the dynamically added capabilities- a form of scope creep. Scope creep is negative if requirements change out of control. When properly controlled, it can be very beneficial from an environmental, economic, security and therefore also ethical perspective. From the points of view of trust and transparency, we need methodological approaches to changing purposes of existing systems. The Waterfall model also lacks these.

Methods such as SIMILAR and TOGAF [44] are better suited for a TACTICS system. They take all relevant phases of the life cycle of systems into account. Both SIMILAR and TOGAF have a cyclical structure, which should keep control of changing requirements, and therefor prevent scope creep.

However, the nature of system-of-systems also complicates this aspect. Design processes are typically limited to one organisation. In the context of TACTICS, adaptations may also be needed on the side of the capabilities, which are not owned by the counter terrorism agency:

- Training of citizens and private security forces for how-to-act in the context of a specific terrorist threat;
- Preparing technical interfaces on the side of urban infrastructure;

Methods from the areas of co-development and the construction of Public-Private Partnerships may be useful to address this issue.

With regard to the speed and growth path of a TACTICS system, Rechtin [35] wrote: "*Complex systems will develop and evolve within an overall architecture much more rapidly if there are stable intermediate forms than if there are not.*" Envisioning a development path with stable intermediate forms may be more crucial for the realization of a TACTICS system than the choice of a particular design method.

The stability of an intermediate form can be expressed using *(technical) maturity levels*. The maturity of a TACTICS system can be expressed by a single expression using TRL, as is illustrated in Figure 10. The TACTICS project will deliver a demonstration system in a simulated environment, i.e. TRL=5. For a more detailed description of the maturity of a TACTICS system, it will be necessary to describe the maturity of its main components and of the integration between them using System Readiness Levels, which rely on TRL to describe the maturity of components, and Integration Readiness Levels to describe the maturity of the integration between components.

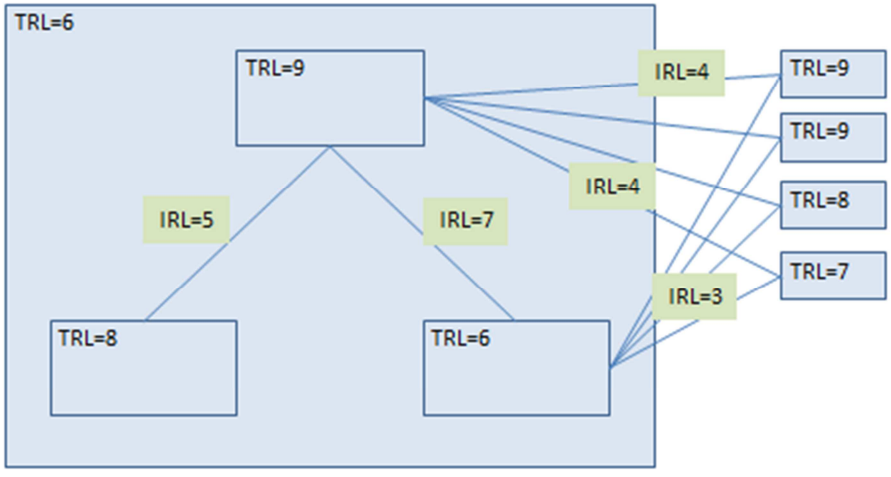


Figure 10 - System Readiness Level can describe the maturity of a system-of-systems. The maturity of the complete system is 6, while the maturity of internal components can be as high as 9. In addition, the maturity of cooperative systems and the maturity of their integration with the core system can be described.

4 Conceptual Solution Description

The TACTICS approach has three pillars:

4) to support decisions with actual, relevant information and to help prevent biases;
5) to dynamically add observation capabilities to the counter terrorism force;
6) to focus on deviant behaviour as learnt from experience with terrorism.

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*. To illustrate the type of work done within these processes, 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 (Figure 11) during the development of a threat (Figure 12):

- The TM is responsible for making decisions based on the complete operational picture;
- The TDM is responsible for providing knowledge on terrorism, terrorist groups and modus operandi;
- The CM is responsible for providing knowledge on the current capabilities that security forces have at their disposal at the threat locations(s).

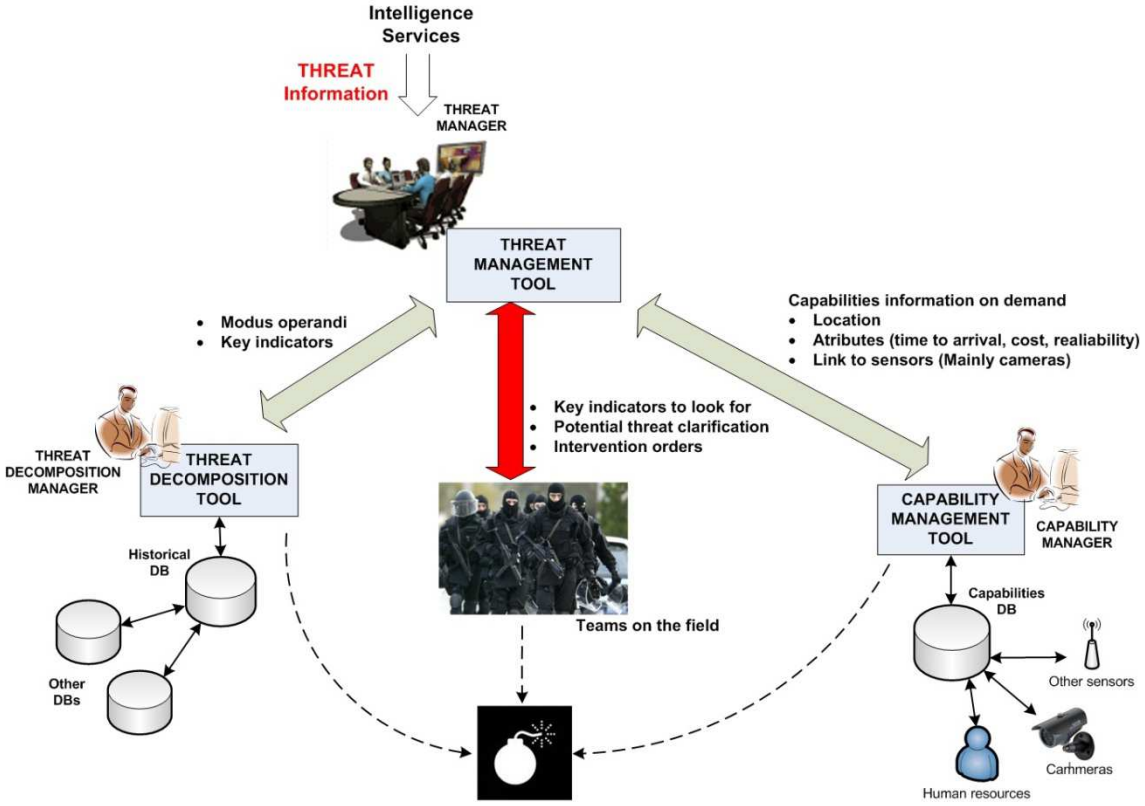


Figure 11 - TACTICS approach

Before the threat has materialized, the focus will be on understanding the threat, and on organizing the relevant capabilities to mitigate the threat. During and after the attack, the focus will shift to preventing and stopping the attack and limiting the consequences.

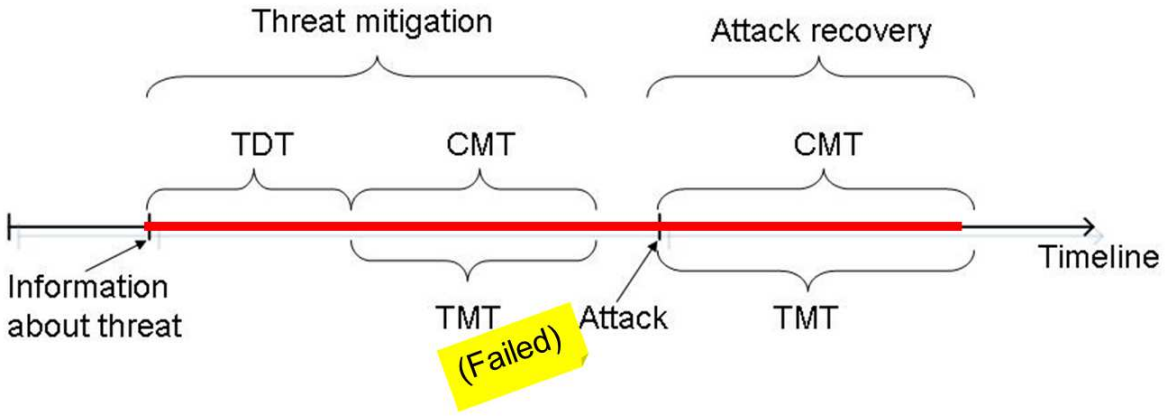


Figure 12 - General activity of roles during threat development.

This approach combines several views on information management systems. The first is the OODA loop [4]. TACTICS enhances the Observe and Orient phases, while the Decide and Act phases are out of scope. TACTICS is a decision *support* system, but does not take (automated) decisions itself. This implies that decisions in the most outer OODA loop are *not* made by the TACTICS system, but by its end user: the commander of the counter-terrorist operation (in the TACTICS project, this role is combined with the threat manager). TACTICS does this by adding Observation capabilities with the Capability Management Tool, and by supporting the Orientation phase with the Threat Decomposition Tool. The Action phase is not part of TACTICS. However, in nested OODA loops, i.e. purely within the Observe and Orient phases, it is possible to request additional information if not enough information is available.

The second view from information management is that of Data, Information, Knowledge and Wisdom [3]. This view is concerned with the use of information. A TACTICS system collects *data* through surveillance sensors which are acquired and integrated by the Capability Management Tool. This data is integrated into information (situational awareness) in the Threat Management tool. Knowledge is created by comparing this situational awareness to potential threats from the Threat Decomposition Tool. This leads to understanding in the head of the Threat Manager. Over the span of several cases, this understanding can lead to wisdom, and vice versa, this wisdom is required of a threat manager in order to make more correct decisions which are in line with ethical and moral codes.

The third view is that of the revised JDL levels of cognitive hierarchy [20]. This view is a much more detailed variant of the OODA loop, and helps to further describe the different kinds of observation capabilities that may be added: transducers, signal enhancers, objects assessment, and situation assessment, or any device which combines several of these.

4.1 Threat Decomposition

The purpose of the Threat Decomposition process is to improve preparedness of security forces by decomposing threats into observable terrorist behaviours specific for urban environments. As the main actor in this process, the Threat Decomposition Manager is responsible for providing knowledge on terrorism, terrorist groups and modus operandi.

Role of the Threat Decomposition Manager:

Before TACTICS	TACTICS approach
The Threat Decomposition Manager has a pile of reports of historical examples of similar threats and a phone list of international experts.	The Threat Decomposition Manager is supported by the Threat Decomposition Tool that gives access to a database with data on threats, modus operandi and behaviour and gives specific queues to look for in the behaviour of urban populations.

Terrorists are known to be adaptive, innovative, and creative in terms of where and how they carry out their attacks. Yet, they are also bound to laws of nature, they have also learnt “best practices” and they have their own morals or “rules of engagement” [15].

If we try to unravel this complexity in a systematic manner, as seen in Figure 5, we can recognize that terrorists target objects (2) and/or subjects (4), and interactions (1,3,5) between these to achieve their objectives. One might consider that destruction of objects (2) and or subjects (4) is the terrorist's prime objective; however, based on the above notions, we can infer that disruption of the (social) system is more likely to be the prime objective and that this is realized by attacking objects and or subjects. Instilling fear is an example of disrupting interactions (5). People who have become fearful behave in a different manner than those who are not fearful. Destroying a hub (2) in a transportation system debilitates the use thereof (1, 3).

Now let us take this systems approach one step further. A terrorist attack is not a single event in time but consists of the choreography of a chain of actions. Historical analyses have revealed a host of choreographies, and knowledge of these is crucial in making sense of pending attacks. We also know that terrorists interact with the target environment prior to the actual detonation of a device. It is these prior (inter)actions that are the focus of TACTICS.

The assumption of TACTICS is that certain terrorist behaviours, which are a necessary part of the choreography of the planned attack, could be detected against the background of “normal” urban interactions/behaviours, and thus could potentially allow for “early” detection. However, this poses a problem in that not all “abnormal” behaviours by subjects in an urban environment are indicative of terrorist behaviour. The mere observation of abnormality is not sufficient reason to assume terrorist intent; confirmation of terrorist intent/behaviour is a necessary next step. This can be achieved by probing actions. By engaging the suspect, and/or engaging the surrounding subjects it is possible to discern ill intent based on the reactions to the engagement.

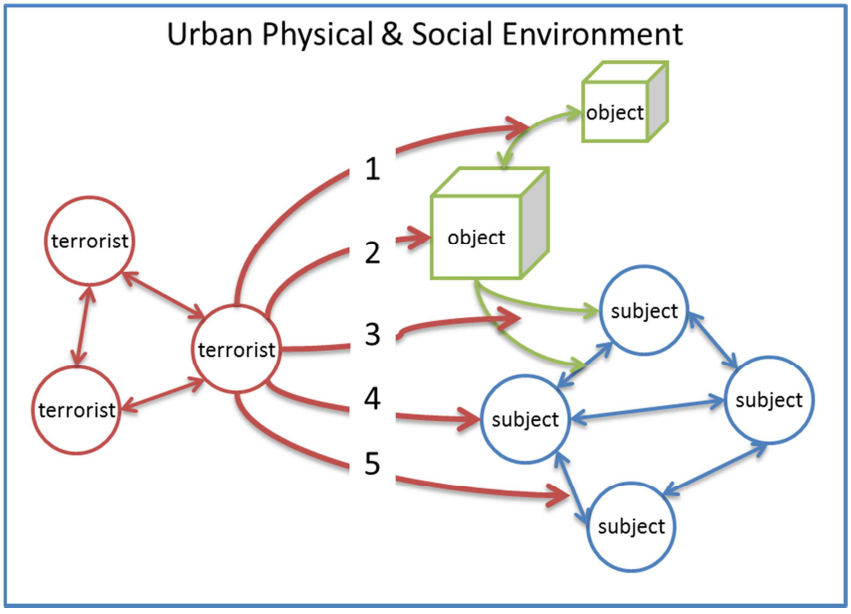


Figure 13- Systematic view of terrorist targeting

There are many ways to orchestrate these detection engagements; what they have in common is the concept of an actuator—a subject or object that (inter)acts and thus can elicit responses that can then be observed by human and/or machine sensors. This actuator can be a person, but also communication devices such as public address systems, video screens, social networking sites, and all sorts of systems that allow for interaction. The elicited responses can then be correlated with the available information to ascertain the likelihood of terrorist intent and facilitate the reduction of uncertainty.

Different cases have shown that security officers can detect terrorists’ *deviances in behaviour*. The UK counter terrorism police investigating the July 7 terror attack spotted the bombers on CCTV as they arrived in London because of their deviant behaviour [43].

Formalizing existing knowledge about threats, modus operandi and behaviour is possible. In fact, the data collection is already on-going business by companies such as RAND, which have built a comprehensive database with historical terrorist plots and attacks.

The method that seems most complete and reliable is defining behaviour by focusing on the common characteristics of all terroristic *modi operandi*. An example of such a common characteristic is the planning cycle. The planning cycles of all terrorist attacks look rather similar and consist of seven stages [15]:

1. Broad target selection
2. Intelligence and surveillance
3. Specific target selection
4. Pre-attack surveillance and planning
5. Attack rehearsal
6. Actions on objective
7. Escape and evasion

Several phases of this planning cycle can be decomposed into observable behaviours that can be detected by humans and technological sensors. This is described in section 4.2 – Capability Management.

A TACTICS system identifies characteristics of different types of urban environments and indicates for a particular type of urban environment the likelihood of specific deviant terrorist behaviour. For example, deviant behaviour decomposed from a threat in which a car bomb is used, has a smaller chance of occurring in a soccer stadium than at a main square.

This is a high dimensional problem with non-quantifiable variables: the urban factors, the threat, modus operandi, weapons and target can all be described in many aspects, but it is difficult or even impossible to quantify them. Table 3 illustrates this with ten dimensions (the columns) with some up to twelve possible values for a terrorist attack with a modus operandi involving a vehicle. The dimensions and values are taken from the historical database from RAND. Such a database can be extended with information extracted from terrorist communications, such as can be found in open source (online) data sources [6]. In fact, the very fact that a particular modus operandi has been shared through open sources might stimulate copycats [42], and may therefore be a valuable dimension to be taken into account. Not only historical scenario's, or scenario's created by real potential terrorists are interesting to add to this database. Also scenario's written by innocent people, such as Hollywood film scripts (if verified on realism by experts) can be valuable to add to such a database. Adding these new scenarios addresses the issue of only being prepared against the "attack of yesterday", and hence increases the quality of information about future terroristic attacks.

Table 3 - Dimensions of a terrorist attack with a modus operandi involving a vehicle.

Threat origin	Types of vehicle	No. of vehicles	Usage of vehicle	Types of IED	Intent	Type of Explosive	Enhancement	Nr of devices	Blast Initiator
Ismalist	Car	1	Vector of attack	VBIED	Suicide	Homemade	None	1	Chemical
Animal extremist	Lorry	>1	Escape	PBIED	Conventional	Civilian	Gas - chemical	2	Electrical
Anarchist	Heavy Plant	No intel	Kidnapping	Letter/ Parcel		Military	Gas - biological	5	Radio
ETA	Tractor		Drive by shooting				Shape charge	10	Mobile signal
IRA	Motorcycle		Obstruction/ Entrapping				Anti-personnel		Flame
	Pedal cycle		Blocking						Pressure
			Transport						Mechanical
			Ramming						
			Trojan Horse						
			Concealment						
			VBIED						
			Decoy						

A morphological analysis (MA) is a problem solving method for high dimensional problems with many non-quantifiable aspects [37]. In such an analysis, the dimensions would be enumerated, and several values for each dimension would be identified. Many combinations would be excluded based on logical, empirical or

normative grounds. The remaining configurations are valid solutions to the problem. A configuration may contain multiple values in one dimension, e.g. a vehicle may be used for both kidnapping and escape. In the example above, a logical exclusion would be suicide and kidnapping, because there would be no one left to kidnap someone. An empirical exclusion –based on the RAND database- could be a tractor delivering a parcel with an IED: this has just not been witnessed before, but might be possible. A normative exclusion might be the use of a bio-weapon by animal rights extremists. Using a MA on the problem of threat decomposition allows the TDM to quickly narrow down the probable threat scenario based on limited initial information. This methods works independent of the order in which information becomes known, i.e. the order of the columns does not matter. This makes TACTICS a decision-support tool that reinforces security forces. The Threat Decomposition Tool can automatically select deviant behaviour, signs and hot spots that are relevant for a specific threat in a specific urban environment by making the connection between deviant behaviour, past and possible future scenarios at a specific urban location. The impact of this tool is to increase preparedness by automatically selecting what deviant behaviour is relevant for security forces to detect in an urban environment. This is done while preventing the TM having to read through thousands of report of prior attacks: this information is presented in a ready-to-use format.

4.2 Capability Management

The purpose of the Capability Management (CM) is to improve the knowledge on the available capabilities at security forces' disposal by improving (1) awareness about the general availability of capabilities most appropriate in a given situation, (2) access to capabilities, and (3) management of capabilities. This is done by automatically matching indicators of a potential threat to available capabilities, such as security staff, camera surveillance or detection of weapons. The matching results in a dynamic overview of most appropriate capabilities, aiming at improved detection circumstances within an urban environment, i.e. increasing the chance for prevention and timely intervention.

Role of the Capabilities Manager

Before TACTICS	TACTICS approach
The Capability Manager has access to the work-schedules of personnel. He gets directions from the Threat Manager where he should focus personnel. He reports back with blind spots and possibilities. He knows which agreements and possibilities are in place at friendly organisations, and the consequences of using them.	The Capabilities Manager uses the Capability Management Tool to manage an ad hoc virtual ICT infrastructure which gives the Threat Management Tool access to information from capabilities. Internally, this tool is concerned with the matching of most appropriate capabilities to the situations to be detected by taking into account, e.g., a capability's location, orientation, accessibility, and up-time. The tool has a geographical view, among other views, and shows per sensor the up-time, location and orientation.

It is obvious that not every urban environment has the capabilities that would be needed to detect the specific signs and behaviours as provided by the Threat Decomposition instantly up and running. Nor do the counter terrorism forces have the knowledge of all potential local capabilities that could be used in case of a threat. For example, most European shopping malls are not equipped with any means for detecting weapons but do have a variety of public and private cameras and security staff. The question is how counter terrorism forces get an overview of what capabilities are (potentially) available at a specific location, and which means would be best suited to detect the specific signs and behaviours in the given situation.

Each capability seems to have its strengths and weaknesses that need to be managed and combined to create optimal detection circumstances [24]. To give some coherent, yet non-exclusive examples:

- Intelligent cameras are better at detecting deviances across large spaces and times compared to what security officers can see. On the other hand, they currently have problems with detecting detailed behaviours.
- Camera operators have the advantage of being able to see more detailed deviances in large spaces. However, a disadvantage is that they are not good at detecting deviances over long periods of time because they have limited attention spans and work in shifts.
- Floor security has the advantage of being able to see very detailed deviances from a very small distance. Also, the people who actually walk around the location are the only sources that are capable of

acting directly after they see something deviant. However, humans are susceptible to biases such as prejudice or stereotyping [24][23][28].

- Databases may have large amounts of information in a form which is easy to process, but they are historical data, not as actual as a sensor would give.

The Capability Management Process is comprised of three sub-processes, which are continuously executed in parallel:

1. Characterize local capabilities with regard to their availability and characteristics;
2. Match threat managers' information need with available capabilities aiming at suggesting a concrete set of capabilities
3. Provide a means to manage capabilities by integrating them into the information flow.

First, security capabilities have to be systematically collected and described in a standardized (machine readable) way. In particular, (1) a systematic collection of potential capabilities will be performed and (2) the capabilities will be described using a capability description language. The characteristics comprise technical (e.g., range, time of operation), financial (e.g., costs per unit per hour), ethical (e.g., level of privacy), geo-spacial (e.g., location), and quality-of-service (e.g. reliability) attributes as well as attributes related to the appropriateness of the capability for detecting currently known signs. TACTICS will do research on the most appropriate methods for characterising heterogeneous information, e.g., by employing an ontology of capabilities. Table 4 gives an impression on some relevant aspects and potential values for them.

Table 4- Relevant aspects when observing threats

Modality	Array Form	Platform	Personal Data	Range/ Distance	Probing	Purpose	Signal Intelligence	Focus of terrorist phase	Cardinality	Cost Total
Radar	Single	Fixed	None	Low-10m	No	Deterrence	None	Broad target selection	0	100
Visible Light	Stereo	Rotating	Observe	Medium-100m	Yes	Preparation	Detection	Intelligence and surveillance	1	1000
Infrared	Wide baseline	Limited Moving	Detect	High-1000m		Intelligence	Classification	Specific target selection	10	10000
Sound		Free Moving	Identify			Prevention		Pre-attack surveillance and planning	100	100000
						Live situational Awareness		Attack rehearsal	1000	1000000
						Investigation		Actions on objective	1.000.000	10000000
								Escape and evasion		

Second, taking into account the actual current information need, formulated by the Threat Manager and based on the output of the Threat Decomposition process, capabilities will be evaluated with regard to their general availability for the local actor and with regard to their appropriateness to provide the required information at a specified level of quality. This matching process is a multi-dimension decision analysis problem with quantitative and qualitative aspects. Despite the obvious combinations like identity/biometrics, behaviour/human CCTV operator, behaviour/intelligent camera's, which are actually included in the TACTICS project, there are others, which require a more detailed analysis. Besides a list of appropriate capabilities, the match can provide hints about what capabilities could be deployed in addition to obtain more accurate information (or in the absence of any capability, any information at all). TACTICS research will yield algorithms for matching capabilities to the threat at hand.

Third, when the capabilities are selected by the threat management, the capabilities have to be managed in terms of interoperability with the TACTIC's information flow. It is necessary to align semantics and situational awareness, including metadata about the location, availability and other aspects of the resources to be shared. For technical sensors this could be, e.g., URL's, calibration, synchronisation, latency and other

operational metadata. For human officer, this could be, e.g., the roster of working shifts, phone numbers and training and certification information.
Last but not least, network security must be adapted to allow these extra links and the physical connection layer must be created.

For privacy concerns, when actually providing a link to a source of information, the expected added value must be made credible and clearly stated. If the information is not needed any more, the capability has to be released.

TACTICS' methods and technologies will provide means for characterising, storing, retrieving, matching, organizing, indexing and delivering information relevant in the current situation. Furthermore, the technology will facilitate the connection of most prominent sensors involved in a mission to the TACTICS system, allowing to 'sense' physical assets real-time status:

- Assessment whether the capabilities that are needed to detect deviant behaviour are actually available at a specific location in an urban environment;
- Assessment of what kind of capabilities are missing to improve detection circumstances in the urban environment.

TACTICS goes beyond the state of the art by supporting security forces (1) to systematically create an overview of the current capabilities available at urban locations and the capabilities that would be needed, (2) to prevent or deal with an attack, and (3) to create optimal detection circumstances, taking into account each capabilities' strengths and weaknesses.

4.2.1 Aligning goals and procedures with cooperative parties

It is one thing to know which actual capabilities would best address the actual information need. It is another to actually find concrete datasources and suggest concrete data links. The conventional approach of applying local capabilities is to confiscate data, to increase the number of police officers or to install additional cameras under direct control and responsibility of counter terrorism forces such as (military) police. However, these options take valuable time and resources. In an urban environment such capabilities may already be present in other public (e.g. public transport) or private (e.g. retail) organisations, but the interoperability is missing on many levels: technically, syntactically, semantically and pragmatically, due to technical, organizational, ethical and legal constraints.

The TACTICS project addresses the middle interoperability levels. On higher levels of interoperability it is important to align goals and procedures. It is not trivial to get concrete links from other organizations to data sources if they are not under direct control of the counter terrorism forces. On a general note Maier [26] wrote on this issue:

> *Collaborative systems imply very little power in a directing authority, perhaps only the authority to hire an architect and publish a "vision" document or standard. Here the architect must carefully select components and interaction standards that will voluntarily be taken up by the participants. The architect can also attempt to design interaction mechanisms that will reinforce an incentive to collaborate rather than act independently.*

A Public-Private Partnership (PPP) could be a useable governance venture to address this challenge. A PPP is operated and funded through a partnership of government and one or more private sector companies. For the security of critical infrastructure, including terrorist threats, ENISA has written a Good Practice Guide on Cooperative Models for Effective PPPs [12]. Some selected recommendations from this guide are:

Recommendation 1. *Membership of a PPP should offer a clear value proposition for both public and private sector stakeholders.*

Recommendation 2. *PPPs should consider the focus of other organisations to ensure that duplication is avoided and that all areas of the life cycle are covered with appropriate co-ordination and information sharing links.*

Recommendation 4. *PPP should consider the type of threat addressed as this will be a defining factor in shaping the membership and determining* which external links are to be forged.

4.2.2 Additional counter-terrorism technologies

TACTICS allows counter terrorism forces to apply resources which are already present in the local city. D2.1 contains a list of urban infrastructures which may be used in such a way. TACTICS also prepares for cases

where those resources are not enough. Such technologies are typically more invasive in terms of privacy, which is one of the reasons why we cannot expect them to be present in any urban environment. In this section some more specialised solutions are presented in the general order of their introduction for the purposes of counter-terrorism in an urban environment.

4.2.2.1 GPS tracking devices.

GPS tracking devices can be used to unobtrusively follow terrorist suspects, and also to locate the security resources such as police cars and personnel. They are typically placed on vehicles or in supplies, and transmit –or store for later reference- its actual location. TACTICS as a project researches their use in relevant scenarios.

4.2.2.1 Automatic Number Plate Recognition (ANPR)

ANPR can be used to detect the presence of certain vehicles at a location. It depends on the vehicle carrying a known number plate. TACTICS as a project does not have plans to research the use of ANPR.

4.2.2.2 UAVs

Unmanned Aerial Vehicles (UAVs) have been developed and used for wide range of tasks. In an urban environment they can be used to unobtrusively follow terrorist suspects, to patrol sensitive areas and for reconnaissance. They allow for reducing the risk to a pilot and they are relatively inexpensive to build and maintain. Most UAV's are controlled remotely by a human operator from a ground station but recently autonomous solutions have also been developed. TACTICS as a project does not have plans to research the use of UAV's.

4.2.2.1 Biometrics

The use of biometrics in a counter-terrorism scenario in an urban environment is sensitive. At the same time, biometrics holds a big promise to detect a certain class of terrorist threats. However, which threats these are, when in the development of threat they can be detected, and whether there are no less invasive means to detect those threats in that phase, are open questions. The research in TACTICS may hint on, or even explore some answers to these questions. This requires a process which combines technology-push with problem-pull.

Biometrics can be used to detect the presence of someone based on his physical body. It can be used for verification, identification and also for following persons. The use of biometrics typically depends on a controlled environment w.r.t. lighting, viewing angle and distance, which is why their use in a cluttered urban environment has been difficult so far. TACTICS as a project performs research on this area by investigating the potential efficacy in three use cases:

1) Identification of terrorists (black list) amidst civilians; (what conditions do you need for the enrolment phase?)
2) Recognition of deviant behaviour: visiting the same site multiple times (day 1 is enrolment, day 2 is recognition); should be easier than 1).
3) Tracking based on face recognition, in order to fuse different observations over time and place on one subject;

4.2.2.2 Intelligent camera's: behaviour recognition

Several previous research project suggest that automatic behaviour recognition (behaviour analytics) may be used to detect abnormal behaviour. A single abnormal action seldom means something, so a form of tracking is typically required to build longer chains of actions. TACTICS as a project performs research on this area. Just like with biometrics, this action is both technology push and problem-pull. The TACTICS research project focusses on investigating the efficacy of this kind of technology.

4.3 Threat Management

The purpose of the Threat Management process is to make security forces capable of responding quicker, without being biased in decision making and to be more precise in the kind of information they request and the orders they send out by providing expert knowledge at the fingertips of the professionals of the security services at the time of an actual threat in urban environments.

Role of the Threat Manager

Before TACTICS	TACTICS approach
The Threat Manager is in charge of the operation. His task is to make decisions based on the complete operational picture. He has information on a specific threat. He asks the threat decomposition manager to decompose the threat into observable terrorist behaviour that can be detected at the threat location. He asks the capability manager to give him eyes and ears on the relevant locations. He hears from the Threat Decomposition Manager what the threat is, and what he should look out for. He hears from the Capability Manager what his options are, and where his blind spots are. He combines this information with human intelligence.	The TMT shows for the relevant locations deviant behaviour, and highlights the behaviour that the Threat Decomposition Manager has told him to look out for. This information is accompanied by meta data such as accuracy; this will give him indications about whether he can trust the information that is presented to him. Internally, this tool fuses data from all types of sources, to get to events and behaviours that are relevant for this task. This tool gets the access to the sensors from the CMT. The tool has a geographical view, among other views. It highlights relevant behaviour, instead of individual sensors. The Threat Manager will be supported by knowledge about biases and subjectivity.

The TACTICS approach is information superiority: if the TM knows enough about the whom, when, where, why and how of an imminent terrorist attack, then he is able to prevent or interrupt it. Some of this information may already be included in an intelligence message, but we have to assume that most of it must still be determined. This can be done by direct observation (surveillance, eavesdropping), interrogation or deduction and statistical means. None of these give information of 100% certainty or the highest quality. In addition, the TM has to work in very uncertain and stressful circumstances. Although he has a strong indication of a specific terrorist threat, he may not have the initiative. If nothing serious has happened yet, he may have trouble convincing others of the seriousness of the threat. Some of his options for intervention certainly hinder a lot of bystanders, while they do not guarantee preventing or limiting the attack. A lot of information is at his fingertips –probably too much to completely assess- but time is pressing and errors will come at a high cost.

The Threat Decomposition Process gives information on what to look out for. This also creates a risk, because they may be wrong. The terrorist attack on Mumbai contained a lot of new elements, and elements specifically designed to confuse counter terrorism forces [16]. Therefore, the TM must organize both specific capabilities looking for the signals that the TDM is warning for, and capabilities which give him a broader situational awareness, looking for deviant patterns which may indicate an unexpected turn of events. This comprehensive information strategy will shape his information demand to the CM.

The Capability Management Process determined what capabilities are present at a specific location and which of these capabilities are best suited to detect the relevant information. As a research project, TACTICS focusses on data about behaviour, and on the integration of such data into situational awareness (information), while applying the principles of privacy-by-design.

4.3.1 Deviant behaviour

The focus on behaviour is a return to the core of every security problem: a threat originates because of someone's actions. TACTICS does not focus on identity, on ethnics or other aspects of a person over which he does not have control. Terrorists have a conscious intent to harm society, and they act upon this intent. The task of counter terrorism forces is to prevent or limit the attack, so data, information and understanding of this behaviour is of utmost importance to them.

Based on interviews of experts and literature review we have found nine different definitions of deviant behaviour:

(1) Behaviour which may lead to dangerous and/ or undesired situations, i.e. which threaten the continuity of the processes at the location;
(2) Behaviour which correlates significantly with incidents;
(3) Behaviour which is part of the modus operandi of a criminal act;
(4) Behaviour which has as purpose to gain an advantage for one self at the cost of someone else: unethical behaviour;
(5) Behaviour which is not part of any of the allowed (work-)processes which occur at the respective location or object;

(6) A reaction which does not fit to the stimulus if the intent of the subject were benign;
(7) Behaviour which falls outside the normal distribution of behaviour at the respective location;
(8) Behaviour which is unwillingly displayed due to high cognitive pressure;
(9) Behaviour which does not fit the local social norms, including anti-social behaviour and culturally abnormal behaviour.

In a general sense, these different definitions are either threat-based (1-4), or continuity-based (5-9). This is inline with two of the main police processes: fighting crime and public order managent. It should however be noted that the efficacy of applying some of these definitions (6-9) has not been thoroughly validated. Their application in counter terrorism should therefore not be done lightly.

4.3.1.1 Face to face predictive behavioural profiling

Probing is to watch the reaction of a person to a set of stimuli. In the context of TACTICS, this can be used to get a more detailed assessment of a person's intentions, e.g. when someone behaves statistically deviant, the next step might be to probe the person to assess his reaction. These stimuli can be brought in artificially, or they can be part of the regular situation. The Search Detect React (SDR®) tool from ISCA is specialized in this method. It can be seen as a form of *predictive behavioural (face-to-face) profiling*, because it is applied (1) before the crime is committed, it is (2) looking only at behaviour, and it is (3) a hands-on method in the direct vicinity of the data subject. Depending on the execution, it can vary from minimally invasive when looking at reactions to stimuli which are part of the environment anyway to highly invasive when the subject cannot avoid reacting to a stimulus. Probing can be done by physical interaction with the data subject, but also by means of (digital) communications, e.g. with the aid of social networking or mobile phones.

4.3.2 Data fusion

Within the TACTICS project a Data Fusion Module will be developed that will be used to assess what kind of (deviant) behaviours are actually detected at the specific urban location. This closes the loop with the information that is provided by the Threat Decomposition Tool, and it presents information at an abstraction level that can be compared with human observation. Having automated tools that allow the management and visualization of information from sensors and first responders involved in a mission is a key element in the management of a terrorist attack and in general in dealing with any civilian urban crisis. These kinds of devices help decision makers to create a Common Operational Picture (COP) of what is going on at the operations theatre.

Data fusion in a surveillance context is not new. In fact several good surveillance design patterns –in terms of obtaining information from raw data- have evolved over millennia of security experience and study:

- The surveillance pattern "Threshold Alarm" works on the basis of putting a threshold on the attributes of a single observable. Typical and often implicit reasoning in this pattern is to consider only the presence (or absence) of an entity, e.g. smoke or a person. This pattern is used in situations where a very specific modus operandi is possible (i.e. fire or breaking-and-entering) which allows for highly specialized observation. Continuous human oversight or more advanced (and costly) patterns (such as "Concentric circles of protection") are disproportional with such a specialized risk.
- The surveillance pattern "Subject profiling" predicts (with an error margin) data points about a person or object from multiple other data points describing different aspects of the subject. The data representation scheme must facilitate linking multiple aspects, actions and behaviours to a single agent. As all of these actions and behaviours will (generally) not happen at the same time, this requires functionality such as person tracking and recognition. This may require additional support from the representation scheme, such as the description of an identity, or some other local and unique biometric attribute. In security and surveillance this surveillance pattern is often implemented in border control and object security on people flows.
- When combined with physical barriers, the surveillance pattern "Concentric circles of protection"[9] has the function of containing the threat in compartments. From an information point of view, this pattern considers the presence of entities in an area, or the transfer of a perimeter between two areas. This pattern is typically used in border security, object security and VIP protection. In general, this pattern allows the surveillance system to designate the relation between one entity and another entity that needs

[9] From an information point of view this surveillance pattern is equivalent to "layered security".

protection. At a minimum, this requires a general idea of the asset to protect and the notion of relative locations. With regard to the perceiving components of a surveillance system (i.e. sensors and surveillance personnel), their location should be known in relation to the compartments in order to know to which compartment their output should be attributed.

New surveillance patterns are also emerging:

- The "Bag of Observations" pattern works by indiscriminately (i.e. not taking into account their specific location or entity that they were observed on) combining multiple observations to estimate the situation, i.e. situation profiling. In the surveillance industry this pattern is experimentally used for situations with very difficult reasoning about an individual person: e.g., crowd management, or urban security. In such contexts, a lot of data is available which can be mined for general behaviour patterns. Combining multiple observables facilitates more robust performance than by putting a threshold on a single observable as in Alarm Threshold. On the other hand, this surveillance pattern misses information on the interaction between different entities (e.g., communication or movement patterns), or on the relation between events and actions (e.g., successive actions are performed by the same person, versus by different persons).
- A second emerging surveillance pattern is the "Relationship View". With the surveillance patterns described above, it is not possible to describe all aspects of scenarios with complex behaviour, i.e. behaviour which involves changing relations between multiple persons or objects. In the earlier mentioned surveillance pattern "Profiling" it is difficult to describe the communication between collaborating pickpockets, the subtle interactions of a drugs deal in a city square, or early signs of a rip-deal in an airport. This illustrates the need for a pattern that includes dynamic interaction between entities such as *X can see Y*, *X speaks with Y* and *X follows Y*. A practical example of this has been identified by the FP7 SUBITO project, which concerns left luggage. SUBITO has identified that the relationship "*owns*" between a person and his luggage is essential to model in order to be able to describe a left-luggage scenario.

4.3.3 Decision support and preventing biases

The concerns with regard to new surveillance technologies are valid: the solutions as described in this report go beyond traditional surveillance, so they raise additional legal and ethical issues which cannot be covered by existing privacy measures.

Given that decisions and preferable actions are very specific to the situation at hand TACTICS will not automate the decision-making process itself. A TACTICS system supports the decision making process by offering ways in which one can decrease risks in the decision-making process. In this case, offering ways in which one can decrease stereotyping, prejudices and conformation bias decreases the probability of the occurrence of false positives and false negatives [27].

Several studies show the risks of the decision-making process in determining if someone is really suspicious or not. There are two essential characteristics of the biased judgment of another person, of his/her intentions or overt behaviours, especially when that person differs in some respect form the judging observer [29]. These are:

- Prejudice: a negative prejudgment of a group and its individual members
- Stereotype: a belief about the personal attributes of a group of people.

Once a stereotype or a prejudice is formed, *confirmation bias* can increase (possibly unjust) negative feelings about a person. Confirmation bias is a tendency for people to favour information that confirms their preconceptions or hypotheses regardless of whether the information is true [34]. As a result, people gather evidence and recall information from memory selectively, and interpret it in a biased way. This leads to the fact that research results show that there is a strong tendency for operators to target males, those in their twenties and black people [32]. In particular, a tracking system facilitates confirmation bias [31] because a tracking system makes it more easy to keep looking at someone who did a minor deviant act. This is considered case building, i.e. collecting more data on a person who was somehow deviant. It is a bias because it prevents a fair view on all persons under surveillance.

A tracking system may also be influenced by positive feedback. Positive feedback is an effect reinforcing itself. A tracking system which can track people with locally unique characteristics (skin colour, clothing, face type) better than other people, will collect more images of those people. But, an increased number of images on a person can also improve his tracking because the person is imaged from more sides, and / or in a greater variety of conditions (e.g. lighting, camera brand or - configuration). Locally unique people (w.r.t. their appearance) will be more easy to find than people who "blend in".

Surveillance bias is the predisposition to watch over certain types of people more than others, regardless of their factual behaviour, e.g. because of ethnicity, skin colour, sex or age. A tracking and finding people will facilitate acting on this predisposition, especially when the system also facilitates searching or filtering on such characteristics.

The concrete impact of these issues cannot be reliably predicted before more specific designs have been made. Some issues can only be assessed in practice when some functionality is available, especially those which depend on concrete use by operators and concrete appearance of people under surveillance. This means that during the entire design cycle, ethical and legal concerns have to be taken into account.

5 Data Model Requirements

The data model is a critical component of a TACTICS system. Its design must be taken as serious as any of the other components, and as such, it is subject to the design process. A collection of requirements for surveillance metadata schemes is introduced by van Rest [48]:

1) Coverage of relevant domain: one single ontology should cover all concepts which are relevant for the TACTICS domain, i.e. the concepts of the morphological analyses, and the output of the fusion engine;
2) Metadata about the sensor: factors which influence the signal should be described, e.g. location, orientation, refresh rate;
3) Metadata about features/observations: the parts of signals which actually contain atrributable data should be known;
4) Metadata about entities, events, actions and their attributes: the datamodel should cover metadata about observable objects;
5) Metadata about situations and scenarios (relations between observables): relations between objects should be described;
6) Describe goals, hypothetical situations and scenarios: this is required for surveillance systems. In the case of TACTICS this refers to resources which have a degree of autonomy, such as human personnel;
7) Traceability: it should be possible to describe where data is coming from, and to be able to verify this;
8) Uncertainty and alternatives: noise and uncertainty can be introduced in many ways in a surveillance system. The data model should be able to reflect this appropriately.
9) Observation capabilities: the datamodel should support describing the capabilities of surveillance components, in order to support capability management.

More specifically, the data model for a TACTICS system should also support these functions of TACTICS:

- Privacy-by-design: be able to trace back whether the system was used correctly:
  - Logging of access to the TACTICS system;
  - Logging of the coupling and decoupling of additional capabilities;
- Threat management, including:
  - The situational awareness model:
  - Behavioural data, including reactions to stimuli, and models of normal behaviour (prior probabilities of behaviour) in certain locations;
- Capability management:
  - The result of the morphological analysis on capabilities, and on their fitness for detecting threat indicators;
  - Information about additional capabilities, including:
    - The address, access and availability details;
  - Describing the configurations of resources, capabilities (including configuration of the fusion engine) which is used to detect precursors and indicators.
- Threat decomposition:
  - The results of the morphological analyses on threats and behaviours;
- All data relevant for any investigations phase, including data on the decisions made by the counter terrorism forces;

The data model(s) that support the outcome of morphological analysis should be flexible to facilitate the arrival of new threats, changing urban factors and technological progress in the capabilities.

After consensus is reached on the requirements for the data model, the building blocks have to be chosen. A single coherent data model –perhaps built from scratch- may appear desirable, but in practice many small data models already exist, and intelligent database linking and ontology mapping may be more realistic.

6 References

[1] Article 8 of the European Convention on Human Rights (1950)
[2] Baron, J. (2007). Thinking and deciding (4th ed.). New York, NY: Cambridge University Press.
[3] Bellinger, Gene, Durval Castro, and Anthony Mills. "Data, information, knowledge, and wisdom." (2004).
[4] Boyd, John R. "The essence of winning and losing." Unpublished lecture notes (1996).
[5] Cavoukian, Privacy by Design – The 7 foundational principles (August 2009, revised January 2011)
[6] Chen H., Thoms, s., Fu, T. J., 2008. Cyber Extremism in Web 2.0: An Exploratory Study of International Jihadist Groups. In: IEEE International Conference on Intelligence and Security Informatics: 98-103
[7] Council Regulation (EU) No 36/2012 - EUR-Lex – Europa http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:016:0001:0032:EN:PDF
[8] D. J. Solove, "A Taxonomy of Privacy," University of Pennsylvania Law Review, vol. 154, no. 3, pp. 477-564 (Jan. 2006)
[9] Devine, P.G. (1989). Stereotypes and prejudice: their automatic and controlled components. Journal of Personality and Social Psychology, 56, 5-18.
[10] EC, COM(2010) 609 (final), A comprehensive approach on personal data protection in the European Union (November 4th 2010)
[11] EC, undated, Status of implementation of Directive 95/46 on the Protection of Individuals with regard to the Processing of Personal Data http://ec.europa.eu/justice/policies/privacy/law/implementation_en.htm, accessed August 3rd 2011
[12] ENISA (2011), Good Practice Guide on Cooperative Models for Effective PPP's
[13] Estefan, J. A. Survey of model-based systems engineering (MBSE) methodologies.
[14] Habash, G. A Military Guide to Terrorism in the Twenty-First Century, Appendix A Terrorist Planning Cycle, 15 august 2007
[15] Habeck, Mary R., The Jihadist Laws of War, The Journal of International Affairs, Spring 2010 – Number 18
[16] High-Level Enquiry Committee (HLEC) on 26/11, April 2009, *Report of the HIGH LEVEL ENQUIRY COMMITTEE (HLEC) ON 26/11*
[17] ISCA Company website, Search Detect React®, http://www.isca.org.il/, Accessed February 27th 2013
[18] J Gulliksen, B Göransson, I Boivie, S Blomkvist, J Persson, Å Cajander, Key principles for user-centred systems design, Behaviour and Information Technology 22 (6), 397-409
[19] K. Burgoon, R. Parrott, B. A. Le Poire, D. L. Kelley, J. B. Walther, and D. Perry, "Maintaining and Restoring Privacy through Communication in Different Types of Relationships," Journal of Social and Personal Relationships, vol. 6, no. 2, pp. 131 -158 (May. 1989)
[20] Kester, Leon JHM. "Designing networked adaptive interactive hybrid systems." Multisensor Fusion and Integration for Intelligent Systems, 2008. MFI 2008. IEEE International Conference on. IEEE, 2008.
[21] Kimlick, M. (2008). Privacy impact assessment for the Screening of Passengers by Observation Techniques, transportation security administration, Department of Homeland Security.
[22] Langheinrich, Privacy by design—principles of privacy-aware ubiquitous systems, UbiComp2001 (2001)
[23] Lousberg, M. (2009) The smart arm of the law. TNO Magazine
[24] Lousberg, M., Langelaan, S., Wetzer, I. & van Hemert, D. (2009). Monitoring van afwijkend gedrag. TNO-DV 2009 C186.
[25] Lyon, David. 2007. Surveillance Studies: An Overview. Cambridge: Polity Press.
[26] Maier, Mark W. "Architecting principles for systems-of-systems." Systems Engineering 1.4 (1998): 267-284.
[27] McCahill, M. (2002). The surveillance web: The rise of visual surveillance in an English city. Cullompton: Willan Publishing.
[28] Meyers, D.G. (1999). Social Psychology (6th Ed.) Boston: McGraw-Hill.
[29] Meyers, D.G. (1999). Social Psychology (6th Ed.) Boston: McGraw-Hill
[30] MW Maier, E Rechtin (2000), The art of systems architecting– CRC
[31] Nickerson, R.S., "Confirmation bias: a ubiquitous phenomenon in many guises," Review of General Psychology 2(2), 175-220 (1998).
[32] Norris, C & Armstrong, G (1999). CCTV and the social structuring of surveillance. Crime Prevention Studies, 10, 157-178.
[33] Oswald, M. E., & Grosjean, S. (2004), Confirmation Bias, in Pohl, Rüdiger F. (Ed.), Cognitive Illusions: A Handbook on Fallacies and Biases in Thinking, Judgement and Memory (pp. 79–96), Hove, UK: Psychology Press.
[34] Plous, Scott (1993), The Psychology of Judgment and Decision Making, McGraw-Hill, p 233.
[35] Rechtin, E, System Architecting: Creating and Building Complex Systems, Prentice Hall, 1991.

[36] Rest, van et al (2012), Designing Privacy by Design. In: Annual Privacy Forum 2012. Lecture Notes in computer science, Springer (*to be published*)
[37] Ritchey, Tom. "General morphological analysis." 16th EURO Conference on Operational Analysis. 1998.
[38] Sauser, B., Verma, D., Ramirez-Marquez, J., & Gove, R. (2006). From TRL to SRL: The concept of systems readiness levels. In Proceedings of the Conference on Systems Engineering Research. Los Angeles, CA: CSER.
[39] Schwartz, Paul M.; Lee, Ronald D.; & Rubinstein, Ira. (2008). Data Mining and Internet Profiling: Emerging Regulatory and Technological Approaches.
[40] Serge Gutwirth and Mireille Hildebrandt. "Some Caveats on Profiling" *Data protection in a profiled world*. Ed. S. Gutwirth, Y. Poullet & P. De Hert. Dordrecht: Springer, 2010. 31-41.
[41] Serge Gutwirth. *Privacy and the information age*. Lanham/Boulder/New York/Oxford: Rowman & Littlefield Publishers, 2002.
[42] Surette, Ray. Media, crime, and criminal justice: Images, realities, and policies. Wadsworth Publishing Company, 2010.
[43] The Independent, *CCTV reveals calm preparations of 7/7 bombers*, http://www.independent.co.uk/news/uk/home-news/cctv-reveals-calm-preparations-of-77-bombers-2105513.html, Accessed at February 28th 2013
[44] The Open Group Architecture Framework (TOGAF 9.1), Introduction , Section 3: Definitions
[45] TILT, Privacyscan Herkenning Digitale Informatie en Fingerprinting (Dutch for Privacyscan Recognition Digital Information and Fingerprinting) https://www.nctv.nl/onderwerpen/a-z/herkenning-digitale-informatie-en-fingerprinting.aspx
[46] Turnitsa, C.D. (2005). Extending the Levels of Conceptual Interoperability Model. Proceedings IEEE Summer Computer Simulation Conference, IEEE CS Press
[47] University of Bonn – Institute of Computer Science – Communication and Networked Systems, *Definitions of Sensor Data Fusion in the Literature* http://net.cs.uni-bonn.de/wg/sensor-data-and-information-fusion/what-is-it/sdf-definitions/, Accessed January 23rd 2013
[48] Van Rest et al, Requirements for multimedia metadata schemes in surveillance applications for security, Journal of Multimedia Tools and Applications, 2013
[49] Wikipedia, Lemma User Centred Design, http://en.wikipedia.org/wiki/User-centered_design, Accessed January 23rd 2013

Annex A Personas in the TACTICS universe

Threat manager

The TM is responsible for making decisions based on the complete operational picture.

The Threat Manager is in charge of the operation. His task is to make decisions based on the complete operational picture. He has information on a specific threat. He asks the threat decomposition manager to decompose the threat into observable terrorist behaviour that can be detected at the threat location. He asks the capability manager to give him eyes and ears on the relevant locations. He hears from the Threat Decomposition Manager what the threat is, and what he should look out for. He hears from the Capability Manager what his options are, and where his blind spots are. In his team he has analysts who make sense of incoming data. He combines this information with human intelligence. Based on the outcome of the different bodies the Threat Manager must take executive decisions.

Skills

The threat manager has to have an overview of the entire situation in order to make the right decision. Therefore it is important that the threat manager can prioritize information and focus on the most essential decisions that have to be made. Also he must oversee the consequences of decision that are made. The threat manager must continually think one step ahead and direct his staff to focus on certain specific topics that will deliver him valuable and crucial information in order for the decisions to be made at the right moment. In doing so the Threat manager initiates action and therefore takes the lead in preventing problems, creating possibilities and projecting the interests and needs of his/her staff and his/her areas of accountability and responsibility. Because decisions can bring certain risks he must be able to way the pro's and con's and perceive the situation from different perspectives and angles. This requires an analytical thought process.

Due to the nature of the field in which the threat manager is acting he must be able to act calm during stressful situations and be able to resolve issues in a short timeframe.

The threat manager must ensure that his decisions are clear and cannot be misinterpreted by the staff members that have to delegate the orders or execute them. He must also be able to follow his instincts and decide that the outcome of (part of) the tool is not sufficient. This due to the fact that he will be responsible for the overall outcome. In order to do so the Threat manager must have the skills to rationally explain and document his decision making process.

Behaviour patterns

Due to the fact that the Threat manager is not only in charge of the operation but also responsible for the outcome he will show a hands-on mentality towards his staff. This means that he will encourage his subordinates to make sure information is delivered complete, in time and in a manner in which he can take direct action. The Threat manager must show a combination of behaviours that are part of a pro-active approach and a reactive approach. The threat manager will act upon concrete information based on situations that have or are taking place but also will continuously be thinking and acting towards future developments. The previous means that the Threat manager will engage in conversations with his advisors: the TDM and CM and be open for suggestions. He will delegate decisions that are not needed to be taken at the highest level.

Capability manager

The CM is responsible for providing knowledge on the current capabilities that security forces have at their disposal at the threat locations(s).

The Capability Manager has the work-rosters of personnel on it. He gets directions from the Threat Manager where he should focus personnel. He reports back with blind spots and possibilities. He knows which agreements and possibilities are in place at friendly organisations, and the consequences of using them.

Skills

The CM is able to analyse the possible capabilities and draw conclusions for the Threat Manager. The CM can advise the threat manager what capabilities should be required given a certain context or situation. He is also able to think ahead towards possible questions regarding capabilities for foreseeable circumstances. Due to the wide variety of capabilities within friendly organisations, and the possible beneficial usage of them, the CM can cooperate well with these partners and motivate them to incorporate the capabilities towards the benefit of the CM. The CM must be able to be creative in incorporating solutions with regards to capabilities. Thinking on an abstract level can open doors to these creative possibilities. Also the CM must

be able to think outside of the box when it considers aligning partnerships, in order to obtain a broad scale of capabilities.

Behaviour patterns

The CM follows the instruction of the Threat Manager and will actively communicate with both the threat manager and the security forces and friendly organisations that can provide the capabilities. The CM will continuously seek to manage the capabilities in an effective and efficient manner. Therefore he will communicate in a direct and interactive manner with the security forces and organisations whereby he must keep an oversight on the possibilities and developments. He will also delegate questions towards the security forces and organisations with regard to capability-specific questions that may still have to be researched.

Threat decomposition manager

The Threat Decomposition manager is responsible for providing knowledge on terrorism, terrorist groups and modus operandi.

The TDM has a pile of reports of historical examples of similar threats and a phone list of international experts categorized by experience with specific threats, modus operandi and behaviour.

Skills

The main skills of the TDM are similar to that of the CM in that he must analyse the outcome of threat decomposition tool and provide the threat manager with the required information and advice. The TDM must have insight in knowledge on the process of terrorism, relevant groups and modus operandi. He must also be able to think of possible variations of modus operandi and know the relevant trends and developments within his field of expertise. Based on a single piece of information the TDM must be able to make a link to possible threat-scenarios. A certain degree of creativity is also an important requirement with regards to possible new (and realistic) modus operandi. In order for the TDM to be up to date on the previous he must be able to acquire a vast network of professionals that can support him with issues relevant to his task. The TDM must seek to acquire a situation in which the relevant partners are willing to share their expertise with the TDM and also think of possible external experts that can support the TDM.

Behaviour patterns

The TDM follows the instruction of the Threat Manager and will actively communicate with both the threat manager and international experts that can provide the required information. The TDM will continuously seek to find the pieces of the puzzle that can determine the actual (scope of the) threat. Therefore he will communicate in a direct and interactive manner with the experts whereby he must keep an oversight on the possibilities and developments. He will also delegate questions towards the experts to research certain aspects of the threat if their knowledge cannot deliver an answer immediately.

Terrorist

Goals and objectives of terrorists i.e. their organizations differ throughout the world and range from regional single-issue terrorists to the aims of transnational radicalism and terrorism. Terrorism is primarily a psychological act that communicates through violence or the threat of violence. Terrorist strategies will be aimed at publicly causing damage to symbols or inspiring fear. Timing, location, and method of attacks accommodate mass media dissemination and optimize current news impact. A terrorist operation will often have the goal of manipulating popular perceptions, and will achieve this by controlling or dictating media coverage. This control need not be overt, as terrorists analyse and exploit the dynamics of major media outlets and the pressure of the news cycle.

Skills

Before an attack can be planned, an aspiring terrorist group must be organized, funded and trained. Operational security is a critical skill that must be mastered to protect the fledgling organization from infiltration by law enforcement or intelligence agencies.

False identification is required for more than just international travel; these documents are required for domestic travel as well as for commercial transactions, such as buying or renting vehicles, procuring safe-houses and purchasing firearms, explosives and other components of manufactured explosives and improvised explosive devices. Establishing a secure form of communication is also a priority.

Planning the attack is another tradecraft skill, which requires the ability to observe a target, identify a security weakness and then contrive a means to exploit the vulnerability. The best planners devise novel approaches

The specific skills required to conduct an attack can range from constructing an improvised explosive device to marksmanship, to driving a truck or even piloting a jumbo jet. Perhaps the most important tradecraft skill in

the attack planning cycle is surveillance tradecraft, or the ability to observe a potential target without alerting anyone that the target is being watched.

Behaviour patterns

A terrorist will evaluate what force protection measures are in effect in the vicinity of a target and determine a cost benefit analysis. From these analyses and forms of study and surveillance, a terrorist will isolate weaknesses of a target and exploit these weaknesses.

Terrorist groups require recruitment, preparation, and integration into an operational structure in order to conduct terrorist acts. Recruits require extensive vetting to ensure that they demonstrate the ability to succeed in assigned missions and are not infiltrators counter to the group's purpose. Terrorist operational planning focuses on economies of personnel and balances the likelihood of loss against the value of a target and the probability of success.

Police officer on the street

The main goal of police officers on the street is to maintain the safety and security of citizens. In this they are responsible for the protection of life and prevention crime and disorder and apprehension of those who have committed crimes or are about to do so. They also have a social task in helping those who need helping.

Skills

The main skill for the police officer is the ability to use good judgment and be able to solve problems. Not only must an officer but able to judge a situation based on the context. But also handle accordingly. Therefore the police officer must be adaptable and flexible, in order to manage the situation at hand. But also have a high alert for safety and security issues and a good control of impulses, while still being able to act upon their intuition. In this it is necessary that the police officer dares to take responsibility and show a mix of resourcefulness, initiative and assertiveness. Besides the previous the police officer must be able to challenge a multitude of situations simultaneously by manner of multitasking and prioritizing. The police officer also has a social task and must therefore be able to incorporate a certain capacity for empathy and compassion. Due to the hectic situations in which police officers can sometimes operate it is essential they can cope with stress and regulate their emotions. To be able to do the previous it is essential that the police officer builds relationships. Not only with their direct partners in the security and safety branch, but also towards civilians. They can be an essential asset in obtaining the necessary goals. To do the previous the police officer must show a certain degree of courteousness, while still being able to stay cautious if the situation demands this. Cooperation with partners, civilian or not requires the officer to be able to hold an open line of communication by being approachable, honest and respectful.

Lastly it is important that the police officer is able report his findings in such a manner that the information can be exchanged with other colleagues and or partners. This means that the information should be complete and detailed enough for a different person to be able to act upon.

Behaviour patterns

The behaviour of police officers on the street is expected to be alert and wary towards safety and security issues. Police officers tend to mainly focus on people who they suspect due to familiarity, suspicious behaviour or simply the fact that they observe certain behaviour that can be defined as illegal. Not only are they alert towards people but also circumstances that can be potentially dangerous or threatening.

The police officers tend to walk in pairs due to the fact that this has been accustomed for many years. Not only because it is more social for the police officer to walk with a colleague, but it also due to safety reasons. If one officer is busy dealing with a problem the other can either assist or be weary of the surrounding environment.

The awareness of police officers towards suspicious activities (behaviour i.e. situations) in relation to a terrorist attack can differ vastly. This is based on the experience of the individual officer and the context in which he or she is acting. For example just after a recent attack police officers will be on high alert, this is also the case if the venue has been marked as a high(er) security area.

Private security agent

The main goal of the private security agent is to protect a certain location, object or person from hazardous influences. The agent focuses on detecting risk full situations (f. g. deviant behaviour) in an early stage and taking the appropriate measures in order to prevent an unwanted situation. Mostly security agents are uniformed and therefore recognizable. This is beneficial because maintaining a high visibility presence leads to deter illegal and inappropriate actions.

Skills

Just like in the case of police officers the security agent must be able to use good judgement and act accordingly. The main focus of the skills is to detect, deter, observe and report. Within this scope it is important that the security agent takes a proactive approach towards this task. In addition to basic deterrence, security officers are often trained to perform specialized tasks such as control and restraint, operate emergency equipment, perform first aid, take accurate notes, write detailed reports, and perform other tasks as required by the client they are serving.

Because of the fact that the agent is hired by a company he must engage people as the company would deem to be correct. This means that clients must be handled with care and only if necessary must the security agent use his authority.

It is also essential that the private security agent can cooperate with other services.

Behaviour patterns

Due to the nature of the fact that the security agent is (often) hired by a company, they are required to focus on the protection i.e. prevention of crime or deviant behaviour in an area that is designated by the company and in which the security agent has the mandate to act upon. This means that the private security agent strictly cannot act towards deviant behaviour that takes place outside the area he or she is employed to survey and act upon. Of course this does not mean that they cannot signal dangerous i.e. deviant behaviour in the periphery. If they do so they will contact local police forces.

Security officers are often called upon to respond to minor emergencies and to assist in serious emergencies by guiding emergency responders to the scene of the incident, helping to redirect foot traffic to safe locations, and by documenting what happened on an incident report.

In some cases both parties operate at the same location. In these situations the private security agent will handle the less grave situations, and if necessary they will hand the situation over to the emergency services as appropriate. This due to fact that the agent does not have the same authority, means and mandate as the police forces. Although the level of mandate does differ between countries and locations within the country. In certain countries security agents can use handcuffs and weapons. For instance in the Netherlands the only private security that can carry weapons are agents that protect the Dutch National Bank

Socially deviant citizen

Deviance is any behaviour that violates cultural norms. Deviance is often divided into two types of deviant activities. The first, crime is the violation of formally enacted laws and is referred to as formal deviance. This means that the act itself can be seen as criminal behaviour. Examples of formal deviance would include: terrorist attacks, robbery, theft, rape, murder, and assault.

The second type of deviant behaviour refers to violations of informal social norms, norms that have not been codified into law, and is referred to as informal deviance. Examples of informal deviance might include: picking ones nose, belching loudly (in some cultures), or standing too close to another unnecessarily (again, in some cultures).

The socially deviant citizen on whom the project will focus is not engaged in criminal behaviour, but the behaviour itself will be suspicious. The intent of a socially deviant citizen is different than that of the main group i.e. the normal citizen, but also different than that of a criminal i.e. terrorist. The difference between the deviant citizen and the latter is difficult to recognize directly because at first glance the intent of the suspicious behaviour cannot be determined.

Therefore in first instance, the tactics system will be alerted. This due to the fact that it cannot be determined if the suspicious behaviour is actually linked to criminal behaviour i.e. a terrorist threat or simply the fact that the person is acting differently to the rest of his surroundings.

Although the initial signs may be similar, it is important for the tactics system to be able to determine if the person has the intent of criminal behaviour i.e. a terrorist attack. Therefore in second instance, due to the tactics system, the suspicious behaviour of the socially deviant citizen can be specified as not being part of the behaviour of a criminal i.e. terrorist. The previous can be done by combining information from the TDM and the outcome of different capabilities from the TCM. By doing so the behaviour can be monitored and reflected on the situation and thus the intent can be determined.

Socially normal citizen

The socially normal citizen acts accustomed to what is expected and shown by others within a certain context. This context may vary by person, time, space, situation and/ or cultural beliefs. The behaviour shown is seen as normal when it is perceived as consistent with the most common behaviour given the

context. The behaviour of a normal acting citizen can often be recognized in contrast to persons acting abnormal. Often this is linked towards normal behaviour being portrayed as good i.e. just and abnormal as being bad or deviant in both the formal and informal sense of the definition. Normal behaviour is often not explicitly noticed, because the vast majority of citizens act normal. Therefore the focus of people is mostly towards the non-confirming, abnormal behaving person.

Behaviour patterns

A socially normal citizen will abide the law and will confirm to informal rules and regulations that may vary given the context. This means that they will not willingly put themselves in danger and will also not be found at locations where they should not be. They have a certain legitimate goal and act accordingly. When questioned upon the citizen will be inclined to respond in a positive matter, whether questioned by formal bodies or not.

Within an urban setting the socially normal citizen will show a variety of behaviours depending on the nature of the presence. Most people will be travelling from a location to another location. This can be between their house and work. But also between different locations for leisure purpose. For instance shopping, and going out for dinner. The normal behaviour is not to linger at a location without a concrete goal. People are mobile unless they arrive at a specific location for a specific goal.

With regards to clothing people will dress according to the type of weather it is and the ‘dress code’ that suits their activity. This can differ from person to person and from activity to activity. Also cultural aspects must be taken into accord.

Annex B TACTICS Storyline

This annex contains a storyline which is used in a user workshop to set the scene and initiate the creation of ideas. This storyline is not one of the actual validation scenarios. The actual TACTICS validation scenarios are described in D2.3.

Setting the Scene
A city with its regular inhabitants.

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.

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.

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.
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 area's 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 ---

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.
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.

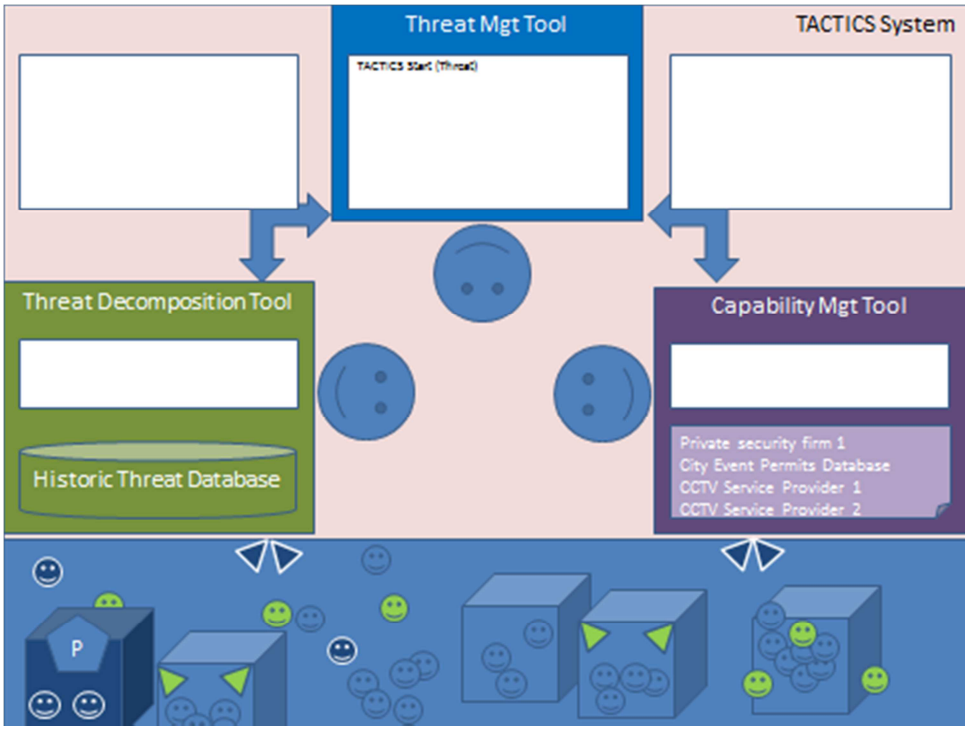
--- start of message ---

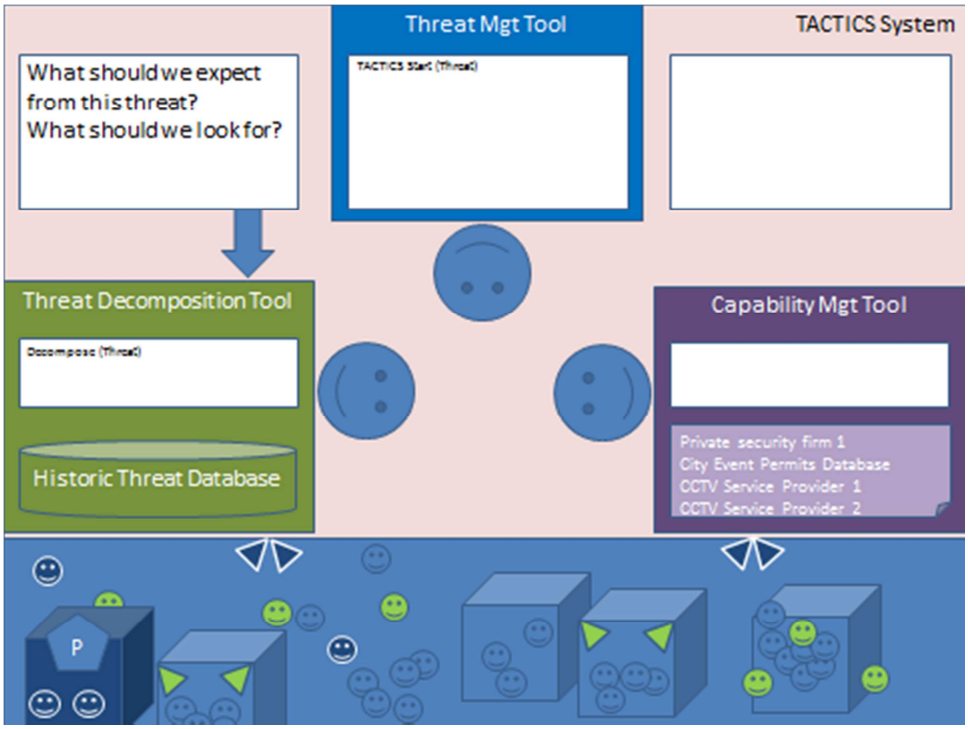
Source: Secret Service

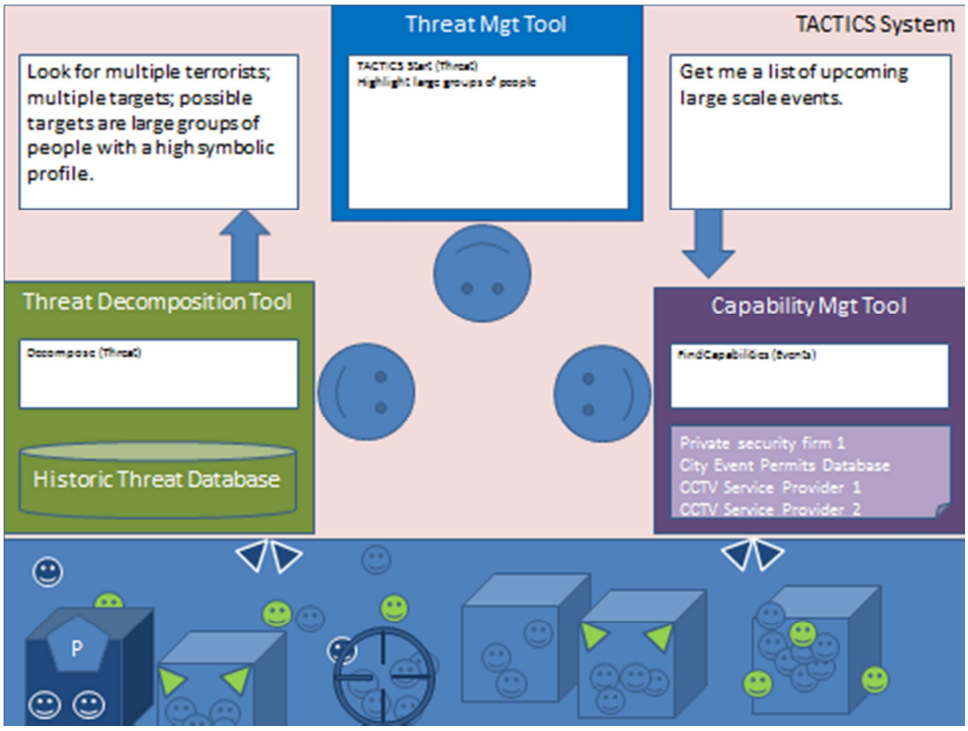
Subject: Urgent Intelligence Report

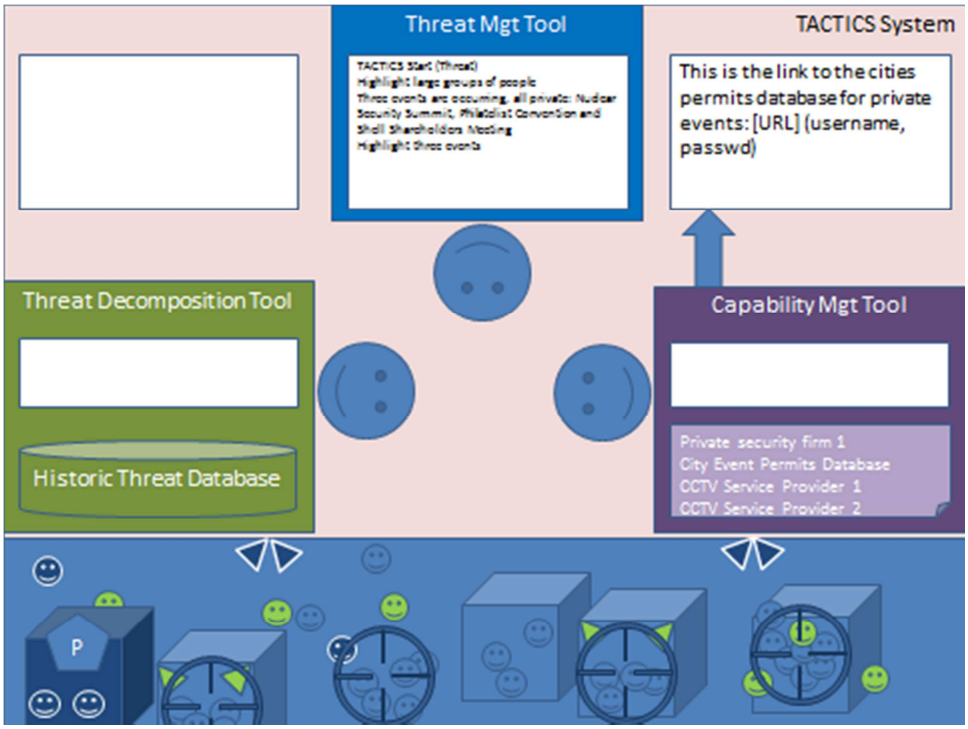
Message: Al Qai'da operatives are referring to imminent drop of a large stash of firearms and explosives in the city of The Hague.

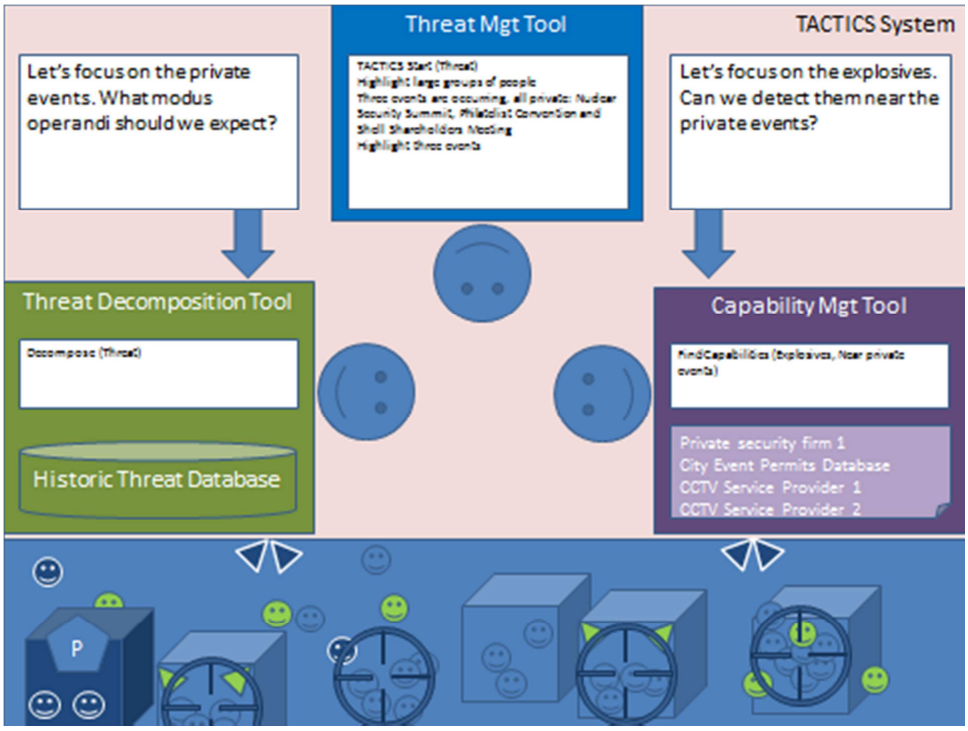
--- end of message ---

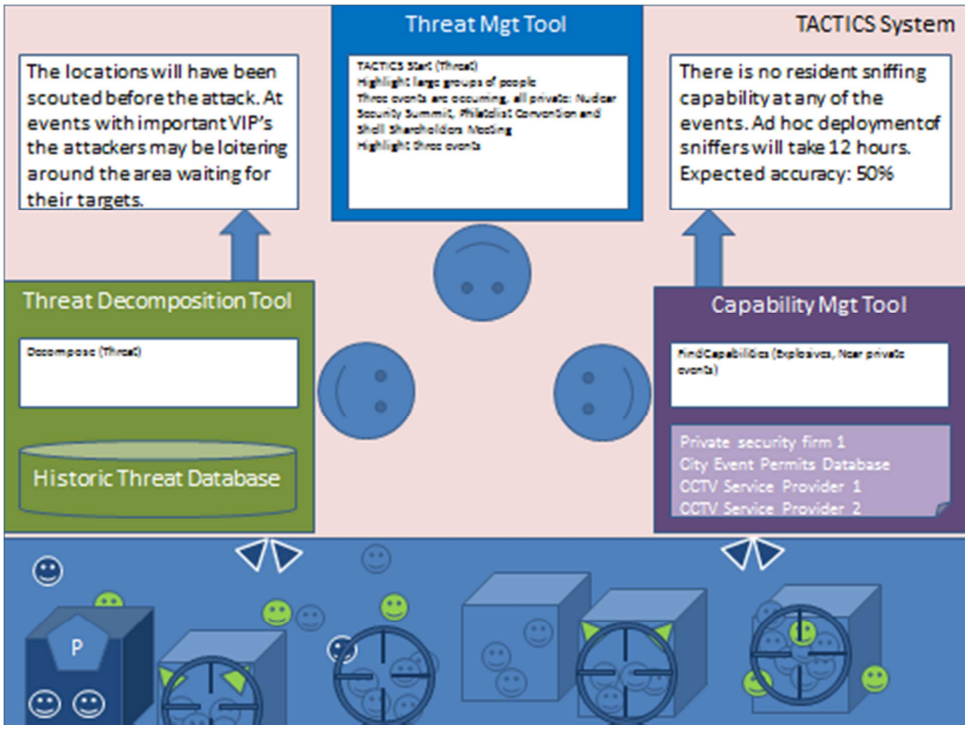

Threat Mgt Tool
TACTICS System
Threat Decomposition Tool
Historic Threat Database
Capability Mgt Tool
Private security firm 1
City Event Permits Database
CCTV Service Provider 1
CCTV Service Provider 2
P


What should we expect from this threat?
What should we look for?
Threat Mgt Tool
TACTICS System
Threat Decomposition Tool
Historic Threat Database
Capability Mgt Tool
Private security firm 1
City Event Permits Database
CCTV Service Provider 1
CCTV Service Provider 2
P


Threat Mgt Tool
TACTICS System
Look for multiple terrorists; multiple targets; possible targets are large groups of people with a high symbolic profile.
TACTICS Start (Threat)
Highlight large groups of people
Get me a list of upcoming large scale events.
Threat Decomposition Tool
Decompose (Threat)
Historic Threat Database
Capability Mgt Tool
FindCapabilities (Events)
Private security firm 1
City Event Permits Database
CCTV Service Provider 1
CCTV Service Provider 2
P


Threat Mgt Tool
TACTICS System
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
Historic Threat Database
Capability Mgt Tool
Private security firm 1
City Event Permits Database
CCTV Service Provider 1
CCTV Service Provider 2
P


Threat Mgt Tool
TACTICS System
Let's focus on the private events. What modus operandi should we expect?
Let's focus on the explosives. Can we detect them near the private events?
Threat Decomposition Tool
Historic Threat Database
Capability Mgt Tool
Private security firm 1
City Event Permits Database
CCTV Service Provider 1
CCTV Service Provider 2


Threat Mgt Tool
TACTICS System
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%
Threat Decomposition Tool
Historic Threat Database
Capability Mgt Tool
Private security firm 1
City Event Permits Database
CCTV Service Provider 1
CCTV Service Provider 2