TACTICS Workshop

Countering Terrorism Threats in Cities

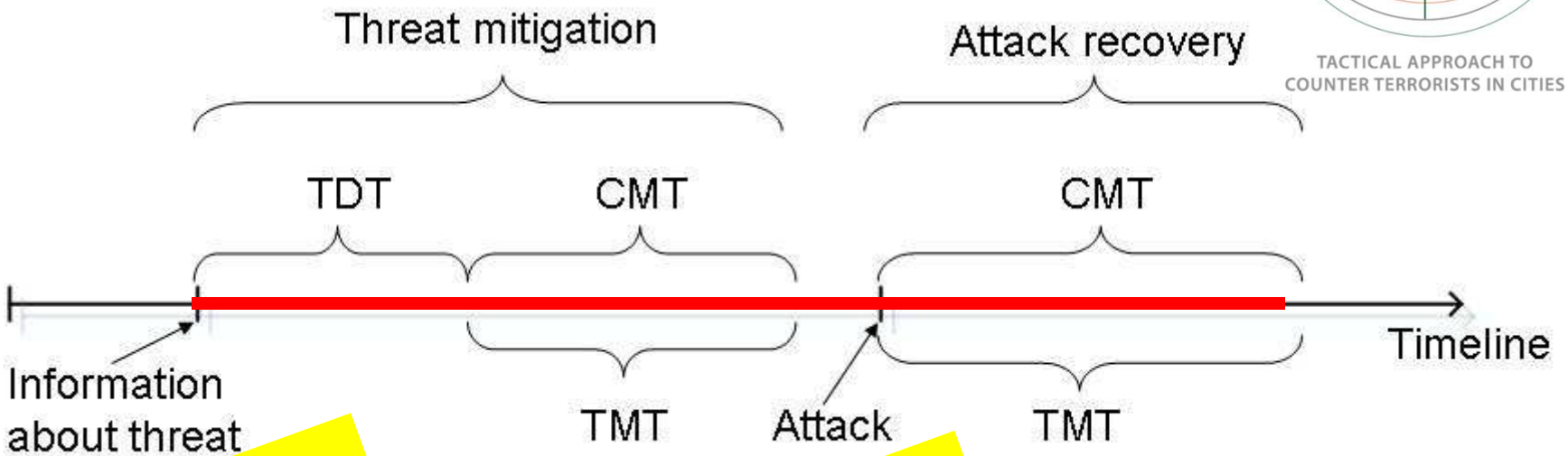
http://www.fp7-tactics.eu

info@fp7-tactics.eu

Oct 2nd , 2014

 Grant Agreement no. 285533

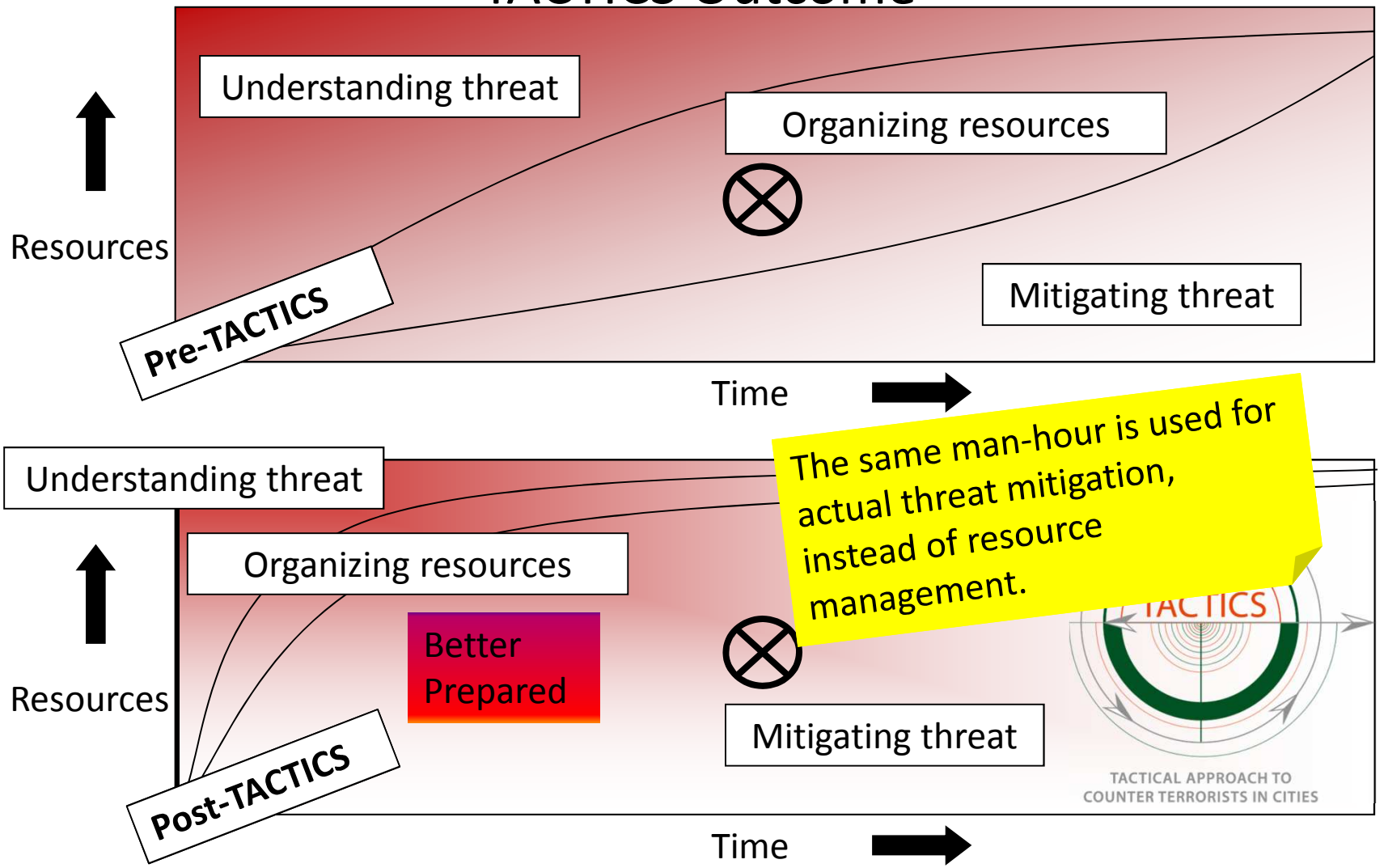
Temporal Decomposition (and scope of TACTICS)



Intelligence information, or signals of a first attack

or failed attack

TACTICS Outcome



TACTICS Project Abstract

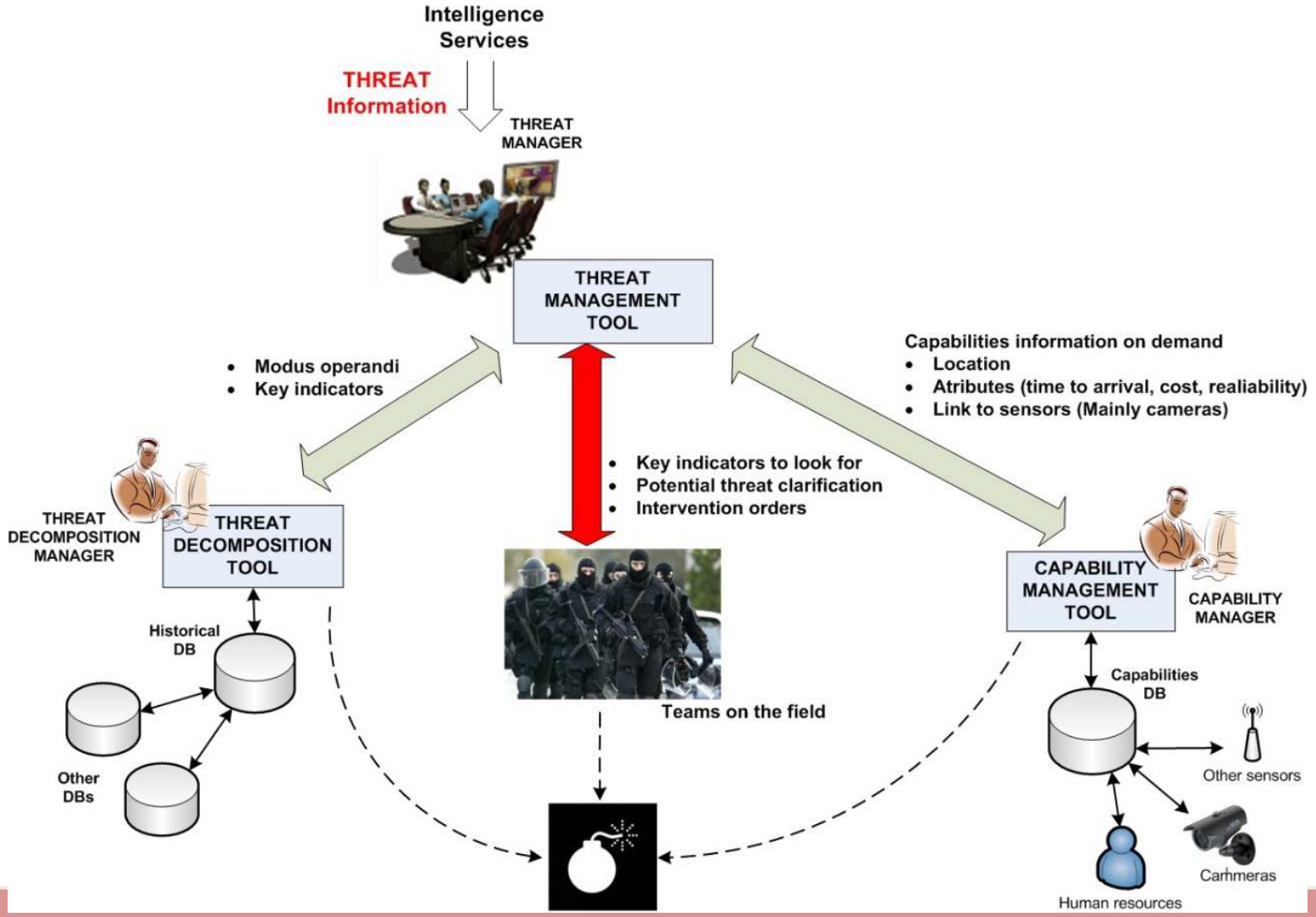
TACTICS seamlessly integrates new research results in the area of **behaviour analysis**, **characteristics of the possible urban-based targets** and **scenario awareness** into a **decision making framework** comprising of **a coherent set of tools and related processes**, supporting security forces in responding **more efficiently and effective** to a given threat in order to **actually prevent the terrorist attack or to limit its consequences**.

Topic SEC-2011.1.2-1 Strategies for countering a terrorist attack in an urban environment

Counter Terrorism: mitigating consequences:

- Insight in threats
- Minimise time to organise capabilities
- As (cost) effective as possible
  - Dual use of existing capabilities and resources, e.g. surveillance with camera's of shopping malls

TACTICS system derived from realistic work process

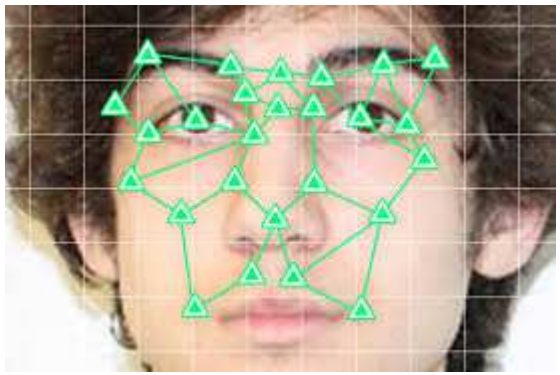


Atomic Surveillance Fusion Patterns

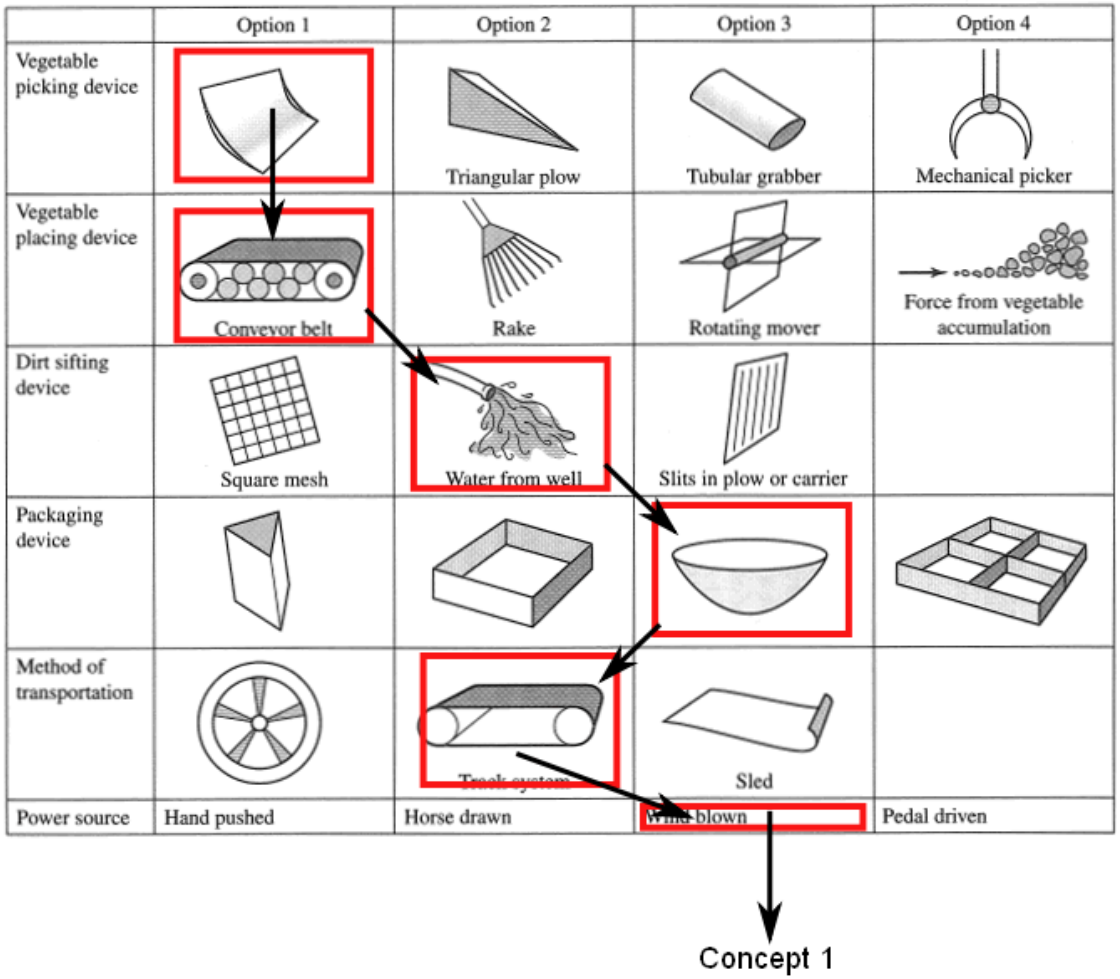
Name	Description	Example
Threshold alarm	A value is going over a threshold	Burglar alarm
Profiling	Extrapolating a value from other values of an object, person or situation	Access Control
Concentric circles of protection	An event is happening in a compartment where it is not allowed	Object Security
Bag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

Set of Tools

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



Overview of possible combinations of modus operandi



Weapon

Target

Modus operandi

City type

Invasiveness

Morphological analysis

Urban environment			
Population density	Climate	Security awareness	Existing infrastructure

Threat decomposition			
Threat origin	Capabilities	Target	Modus operandi

Capability management				
Object to be observed	Sensor type	Platform	Reliability	Invasiveness

Threat assessment			
Intervention phase	Reliability	Criminal phase	Threat dimensions

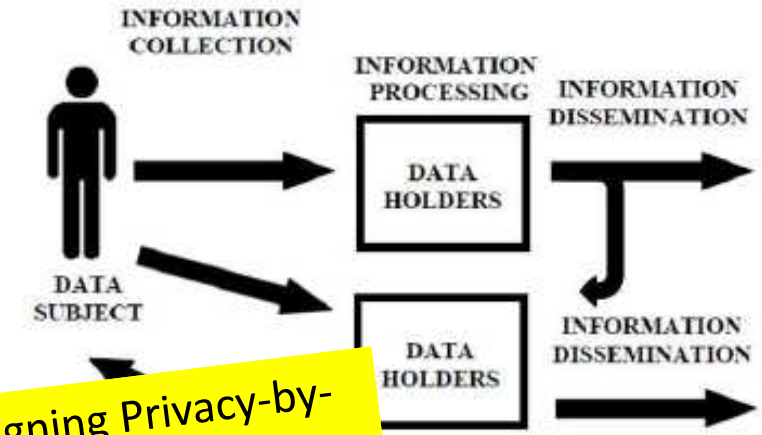
Behaviour

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

Privacy by Design

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 careful consideration and evaluation at the highest and more representative level of policy-making.

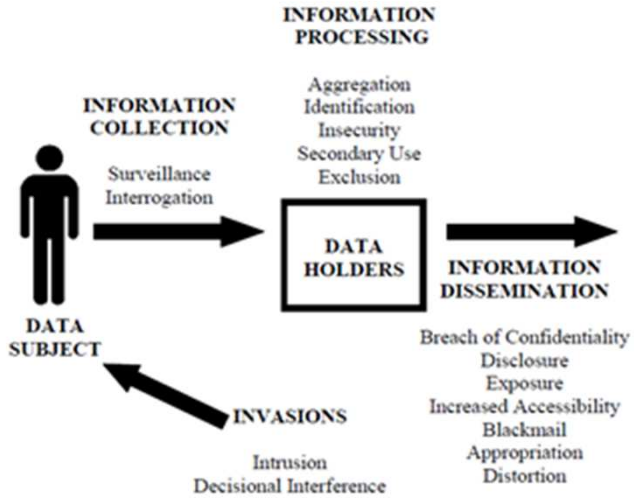
- Follow the law
- (Re)designing Privacy by Design
- Identifying privacy invading activities
- Specifying 7 + 1 principles of PbD
- Methodological approach



van Rest, Jeroen, et al. "Designing Privacy-by-Design." Privacy Technologies and Policy. Springer Berlin Heidelberg, 2014. 55-72.

Invasiveness

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



Solove, A taxonomy of privacy, 2006

TACTICS Beyond State of the Art (1/2)

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

TACTICS Beyond State of the Art (2/2)

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

This need is actual.

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

(European Commission, 2011)

This approach fits actual developments.

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

(TACTICS consortium, 2011)

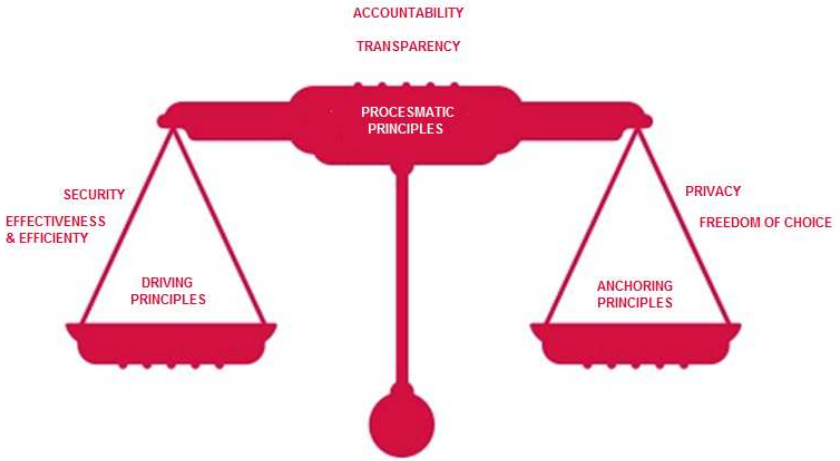
A cross European common approach is needed

There are several reasons for a common approach across Europe:

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

TACTICS is the least invasive approach

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



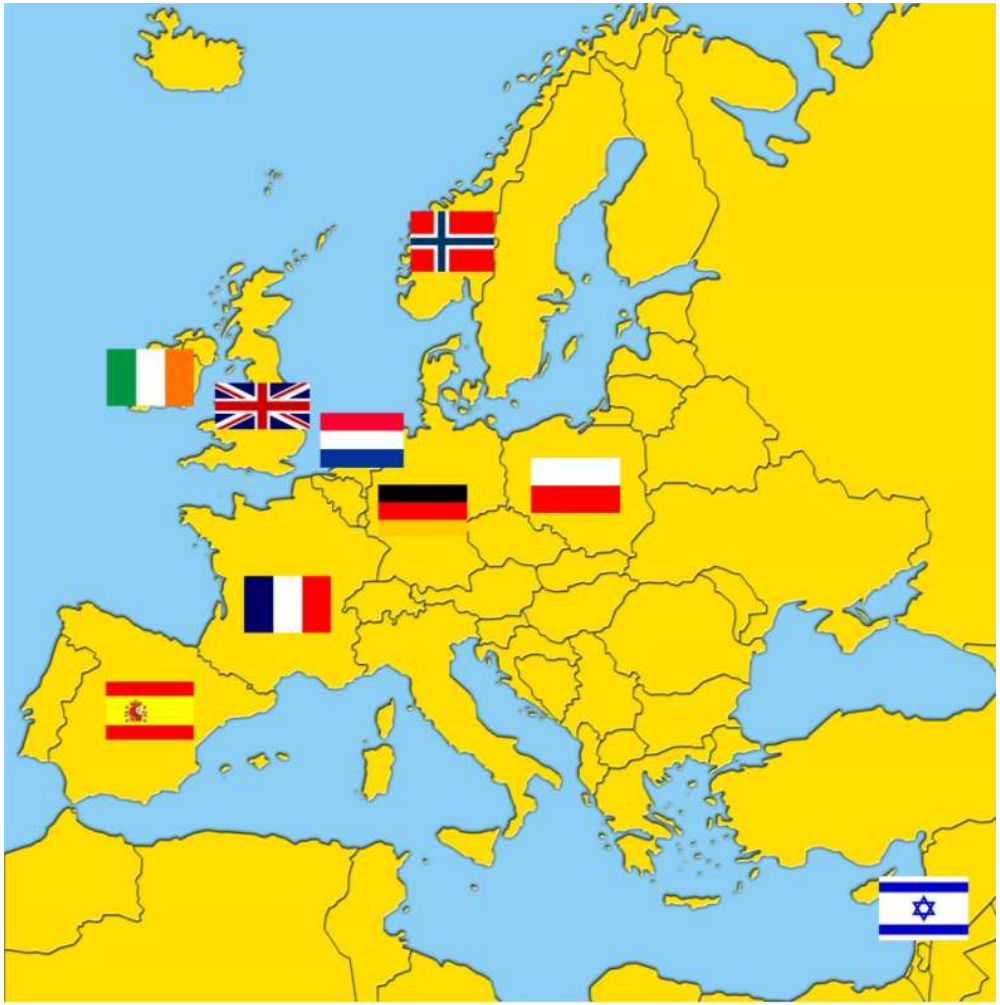
EU Research is valid instrument for this purpose

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

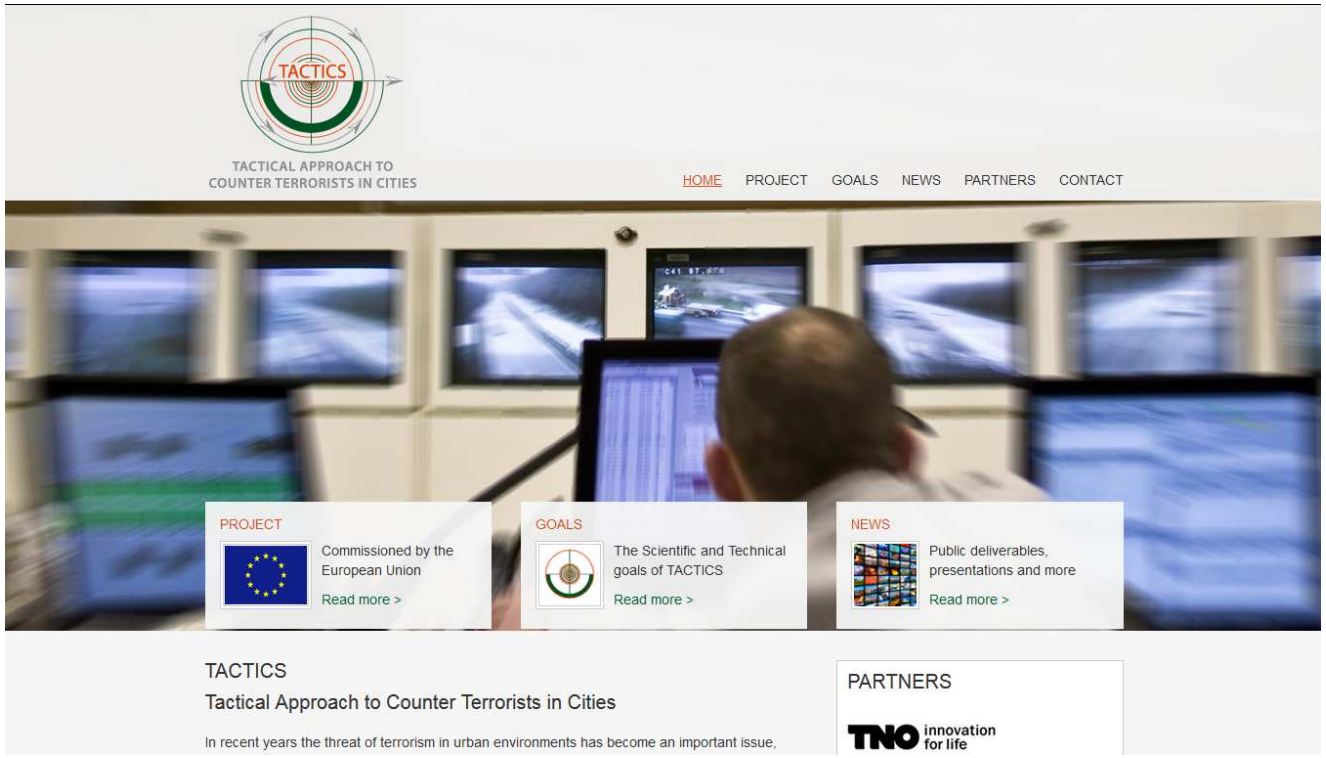
- ensure the security of citizens from threats such as terrorism, natural disasters and crime, while respecting fundamental rights including the protection of personal data
- ensure optimal and concerted use of available and evolving technologies to the benefit of civil European security,
- stimulate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

Consortium

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



Follow us!



info@fp7-tactics.eu

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

References

Selected papers and reports:

- Bouma, Henri, et al. "Real-time tracking and fast retrieval of persons in multiple surveillance cameras of a shopping mall." *SPIE Defense, Security, and Sensing*. International Society for Optics and Photonics, 2013.
- Burghouts, Gertjan J., and Klamer Schutte. "Correlations between 48 human actions improve their detection." Pattern Recognition (ICPR), 2012 21st International Conference on. IEEE, 2012.
- Burghouts, Gertjan J., and J-W. Marck. "Reasoning about threats: From observables to situation assessment." *Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions on* 41.5 (2011): 608-616.
- Rest, J.H.C. van, et al. "Designing Privacy-by-Design." *Privacy Technologies and Policy*. Springer Berlin Heidelberg, 2014. 55-72.
- Rest, J.H.C. van, et al. "Requirements for multimedia metadata schemes in surveillance applications for security." *Multimedia Tools and Applications* (2013): 1-26.
- Rest, J.H.C. van, Roelofs, M.L., Nunen, A.M. van, Deviant behaviour - Socially accepted observation of deviant behaviour for security - extended summary. TNO, 2014
- TACTICS Consortium , D2.1 *Factors Overview*, 2013
- TACTICS Consortium , D2.2 *Requirements Specification*, 2013
- TACTICS Consortium , D2.3 *Scenario Specification*, 2013
- TACTICS Consortium, D3.1 *Conceptual Solution Description*, 2013, http://www.fp7-tactics.eu/
- TACTICS Consortium, D3.2 *System Architecture*, 2013, http://www.fp7-tactics.eu/
- TACTICS Consortium , D4.4 *TDT (Non) Functional requirements*, 2013
- TACTICS Consortium , D5.5 *CMT Functional requirements*, 2013
- TACTICS Consortium , D6.4 *Information Management tool functional requirements*., 2013

Selected patents:

- Den Hollander, Richard Jacobus Maria, Henri Bouma, and Sander Hubert Landsmeer. "System and method for identifying image locations showing the same person in different images." U.S. Patent Application 13/810,219.
- Mark, Wannes van der “Surveillance system and method for detecting behavior of groups of actors” European Patent No. 2568414 A1, 13 Mar. 2013


TNO innovation for life

At least three design phases

1. Proposal phase: Result is proposal (paper)

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

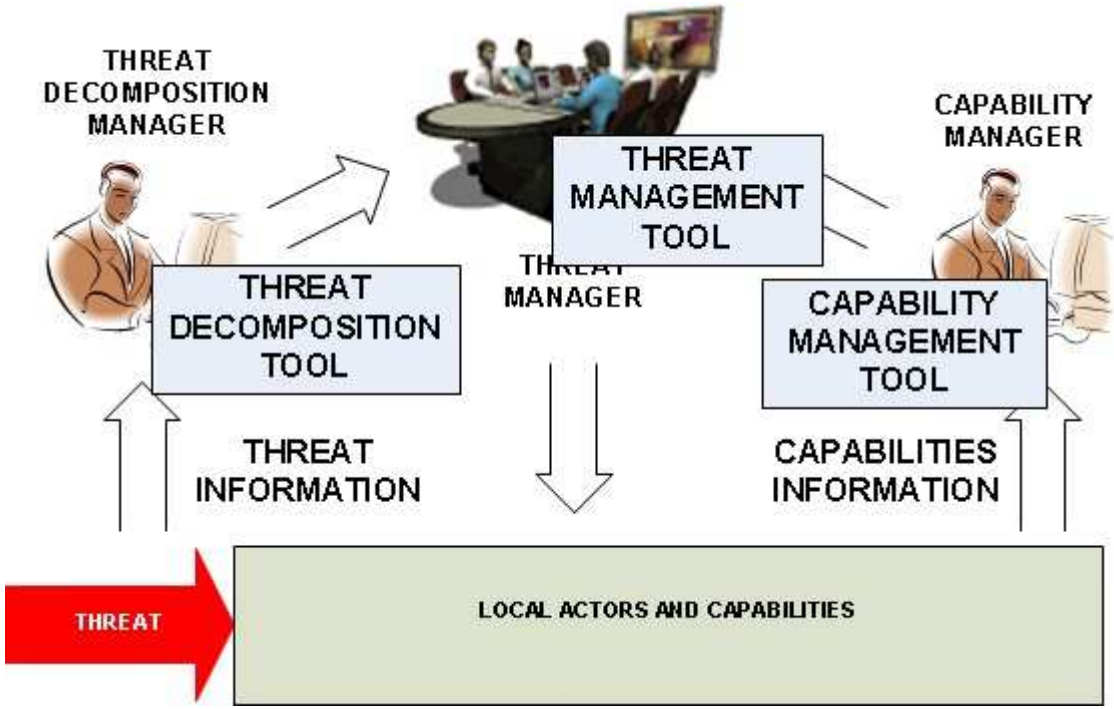
3. Operational integration phase: Result is operational product(s)


TNO innovation for life

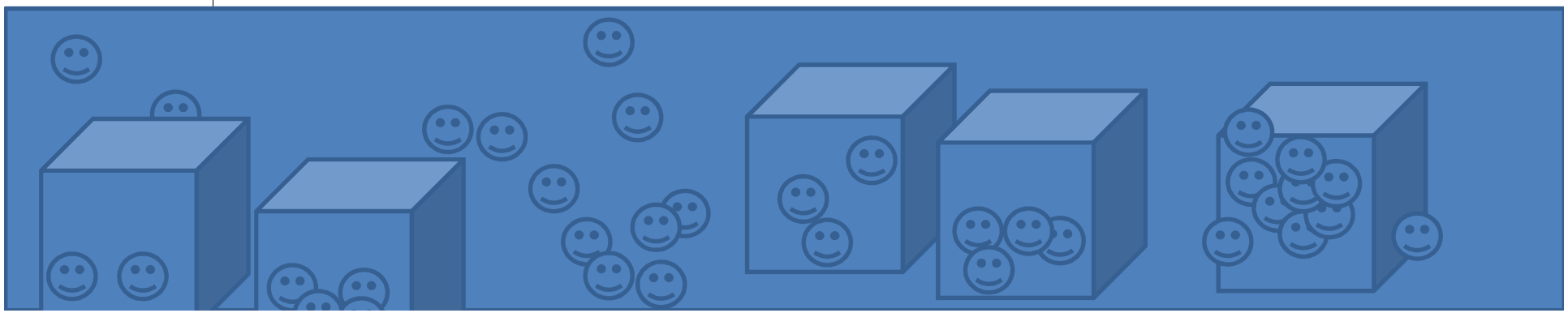
Starting points

- TACTICS System (TS) is a deliverable, but not the main deliverable, it is merely a vehicle to demonstrate several concepts;
- TS is the system that is composed of the TDT, CMT and the TMT. Everything else, also other police systems, are considered “environment”.
- TS Environment includes: city infrastructure; friendly actors and information sources: “regular” security infrastructure, including police forces, private security forces; neutral actors: citizens, other public services; hostile actors: regular criminals, terrorists;
- TS temporarily connects to parts of environment during the development of a threat, and disconnects when the threat is gone;

Functional Decomposition (from proposal)

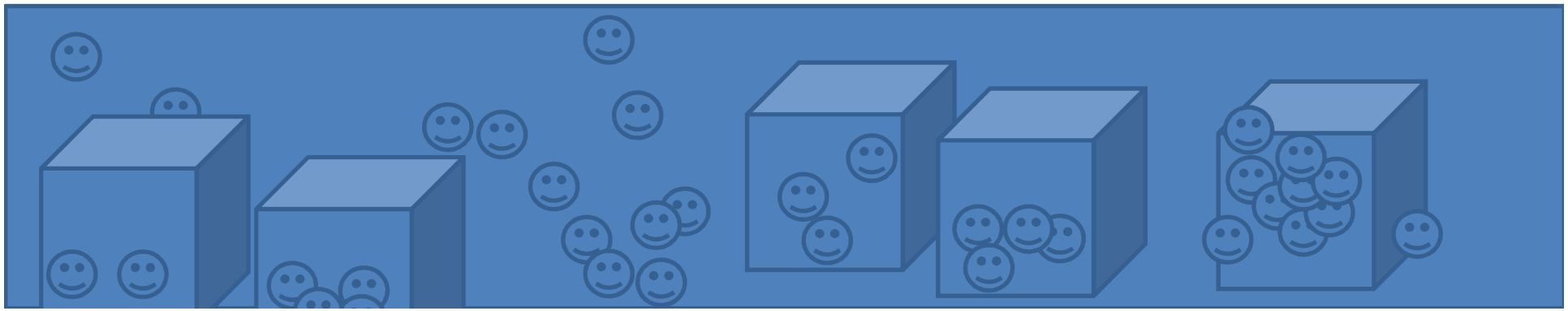


TACTICS Initiation



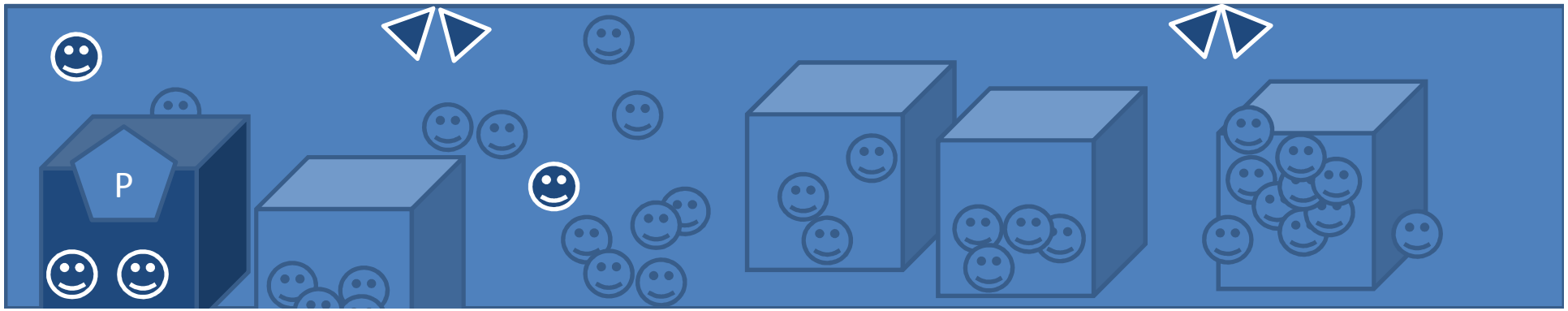
Setting the Scene

A city with its regular inhabitants.



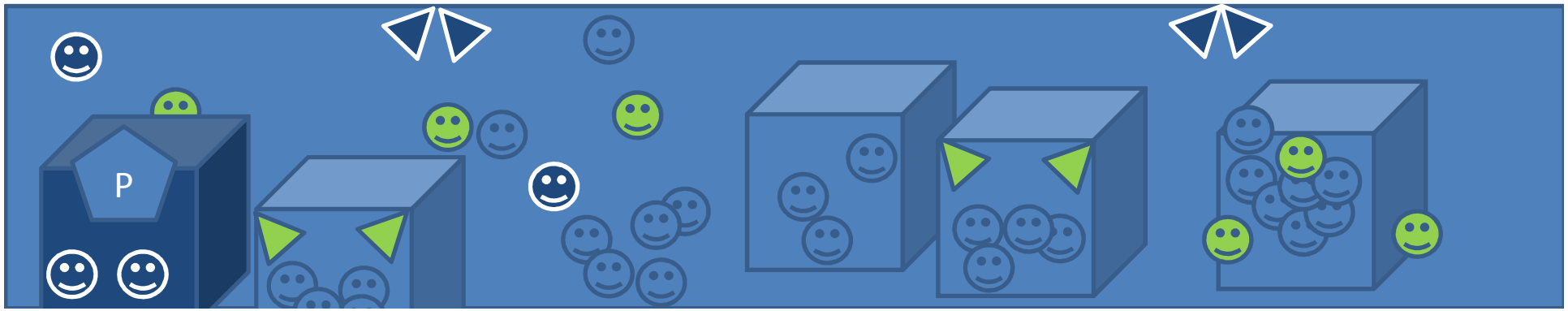
Setting the Scene

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.

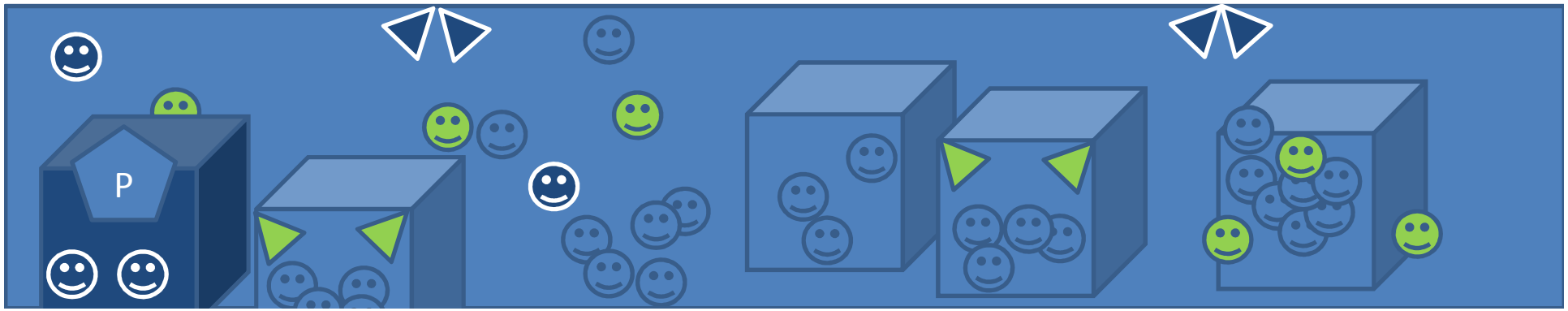
--- start of message ---

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.

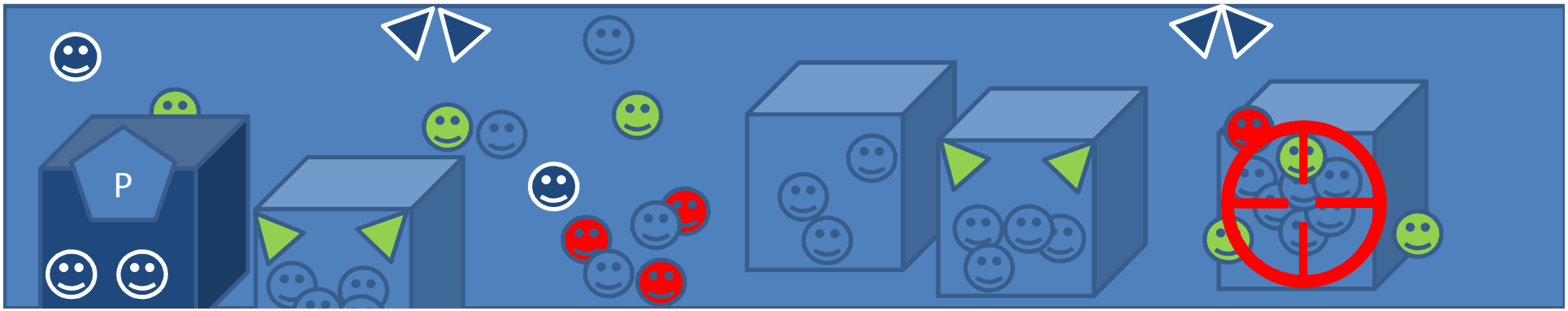
--- start of message ---

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.

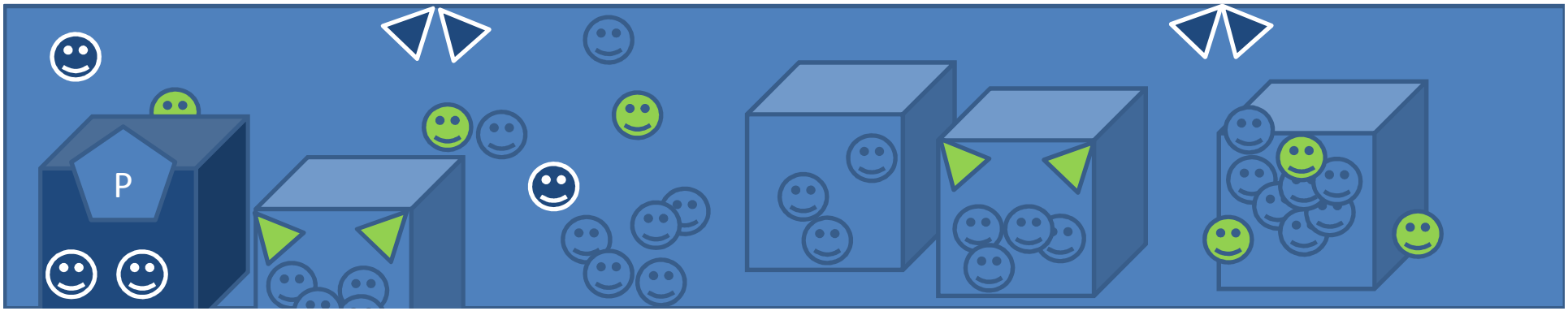
--- start of message ---

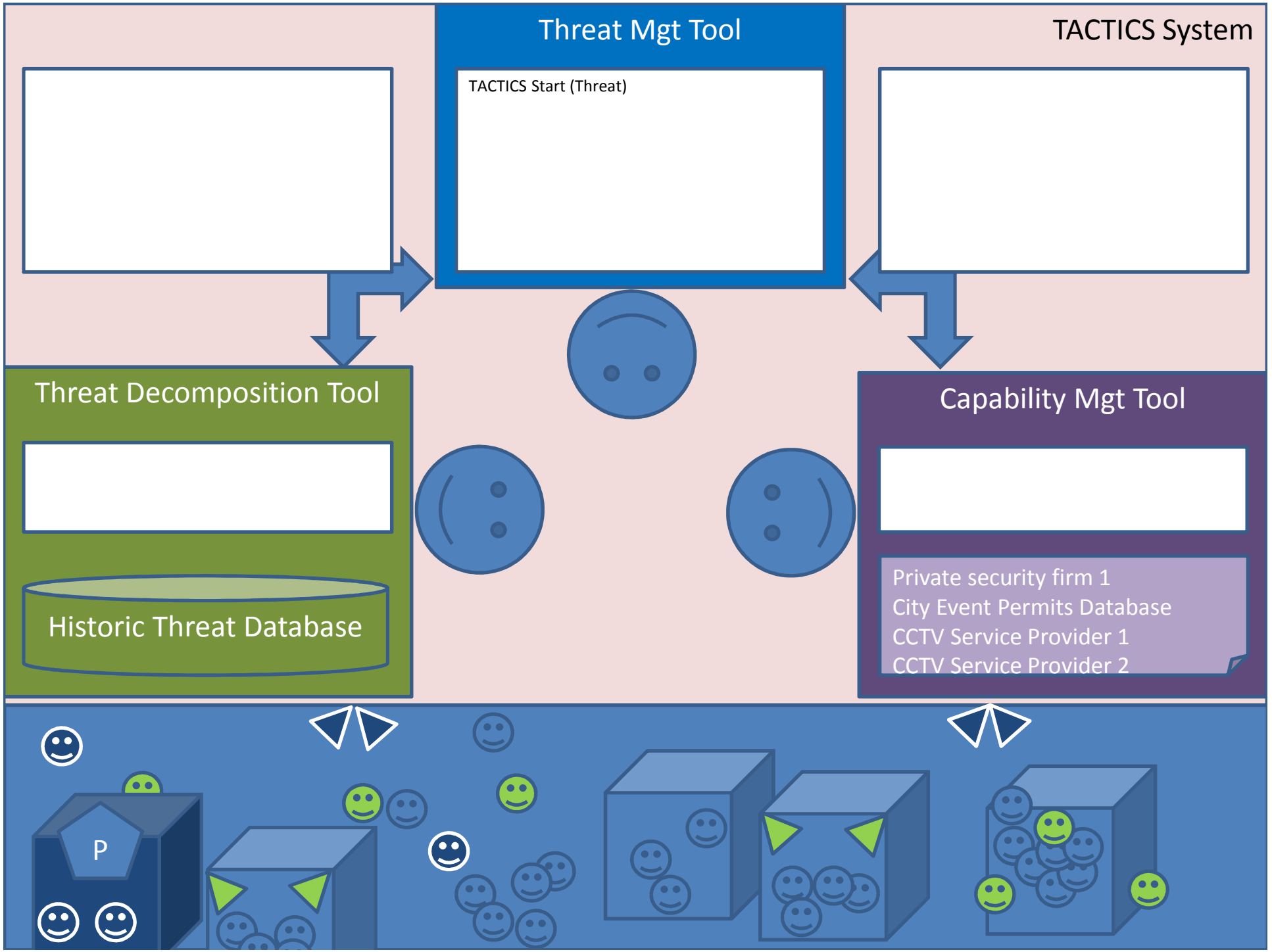
Source: Secret Service

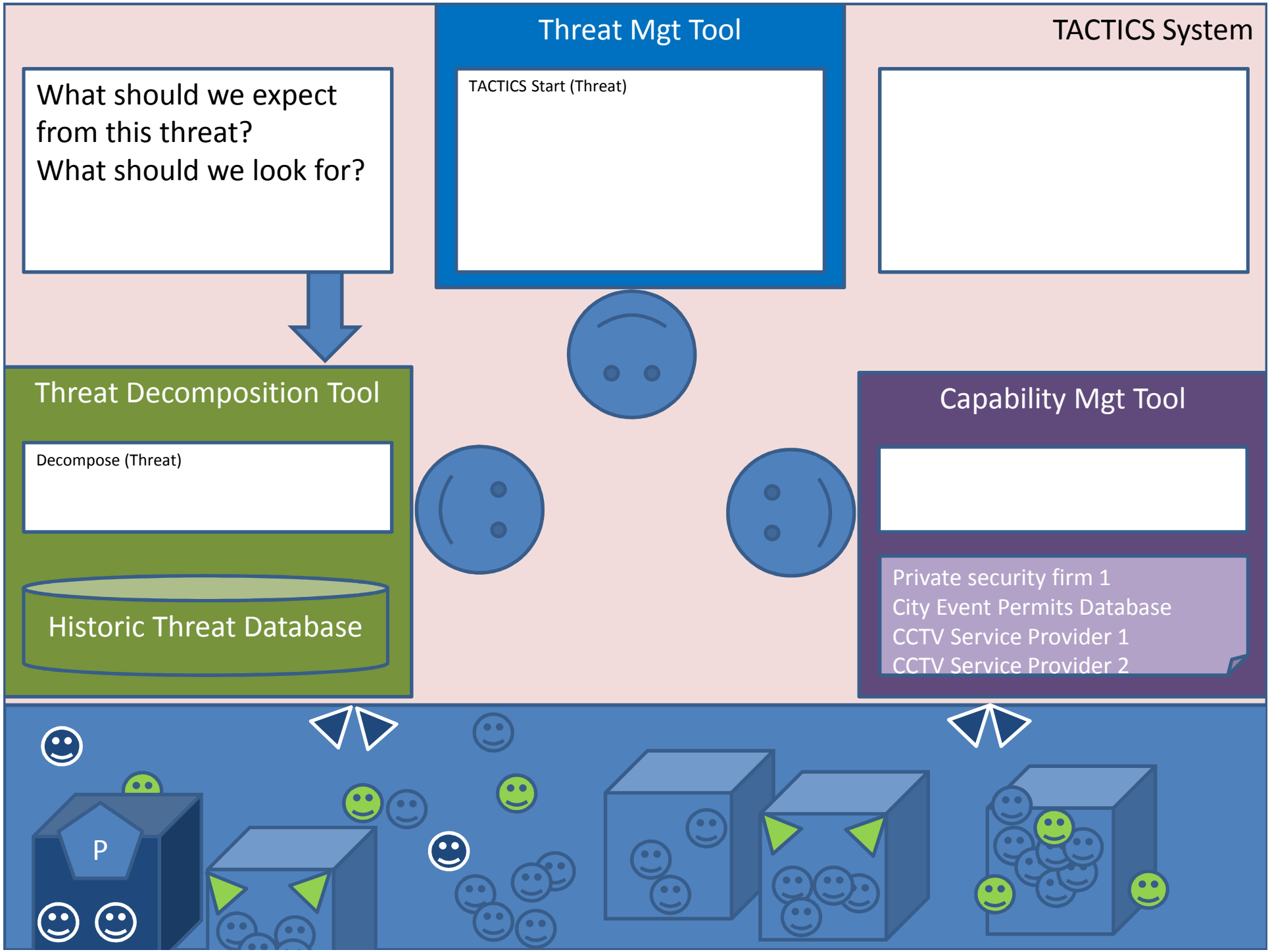
Subject: Urgent Intelligence Report

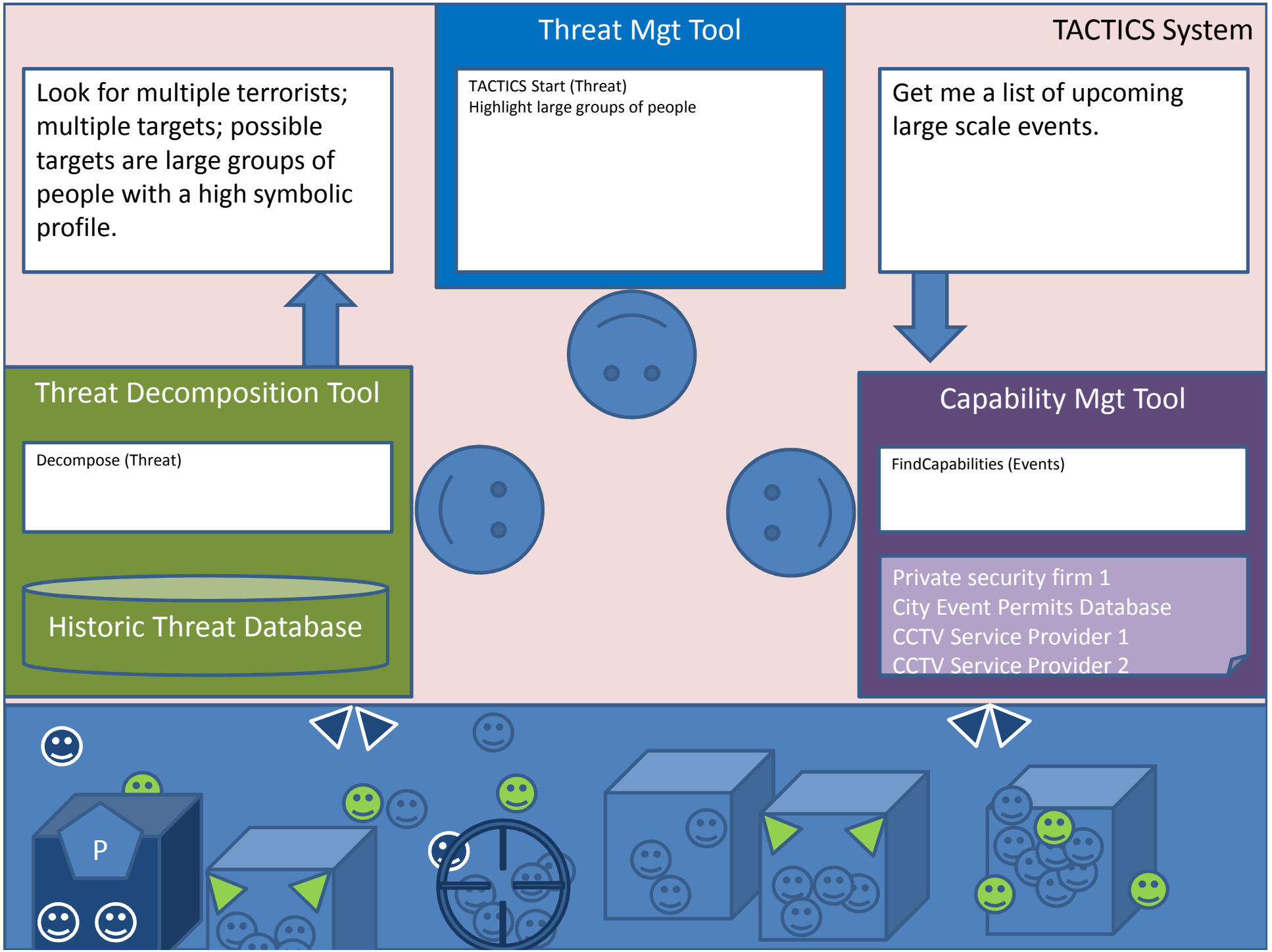
Message: Al Qai'da operatives are referring to imminent drop of a large stash of firearms and explosives in the city of The Hague.

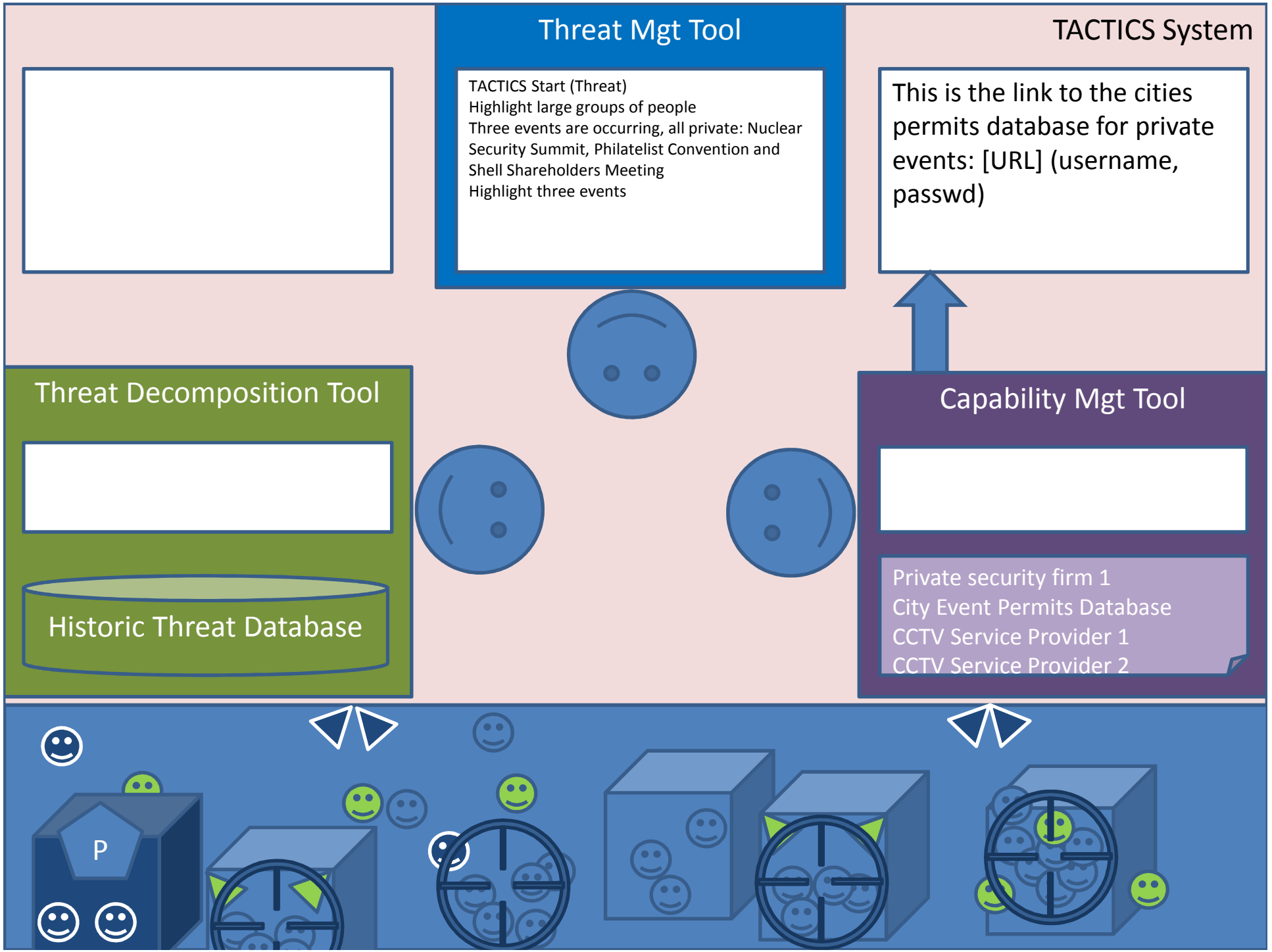
--- end of message ---

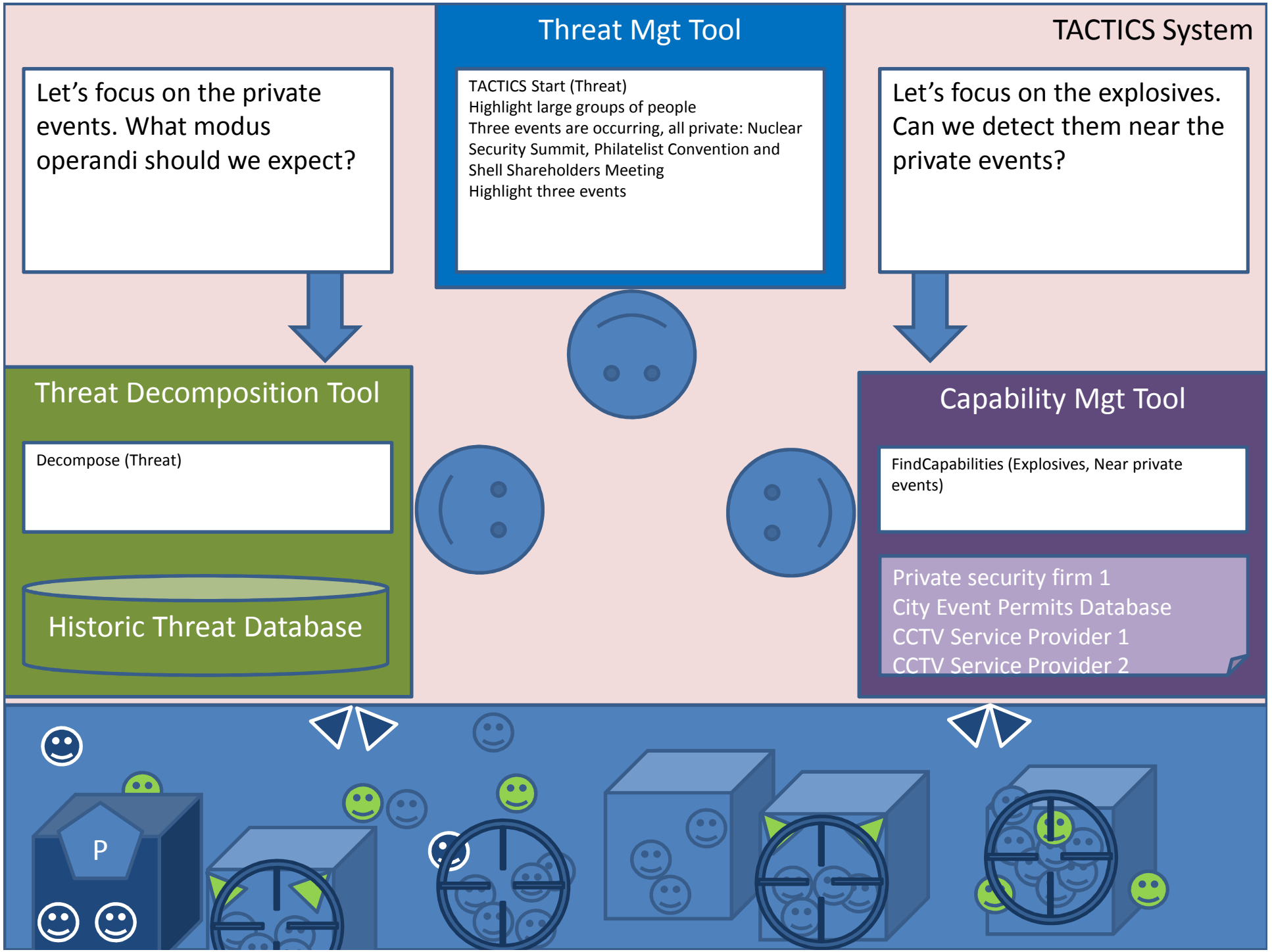


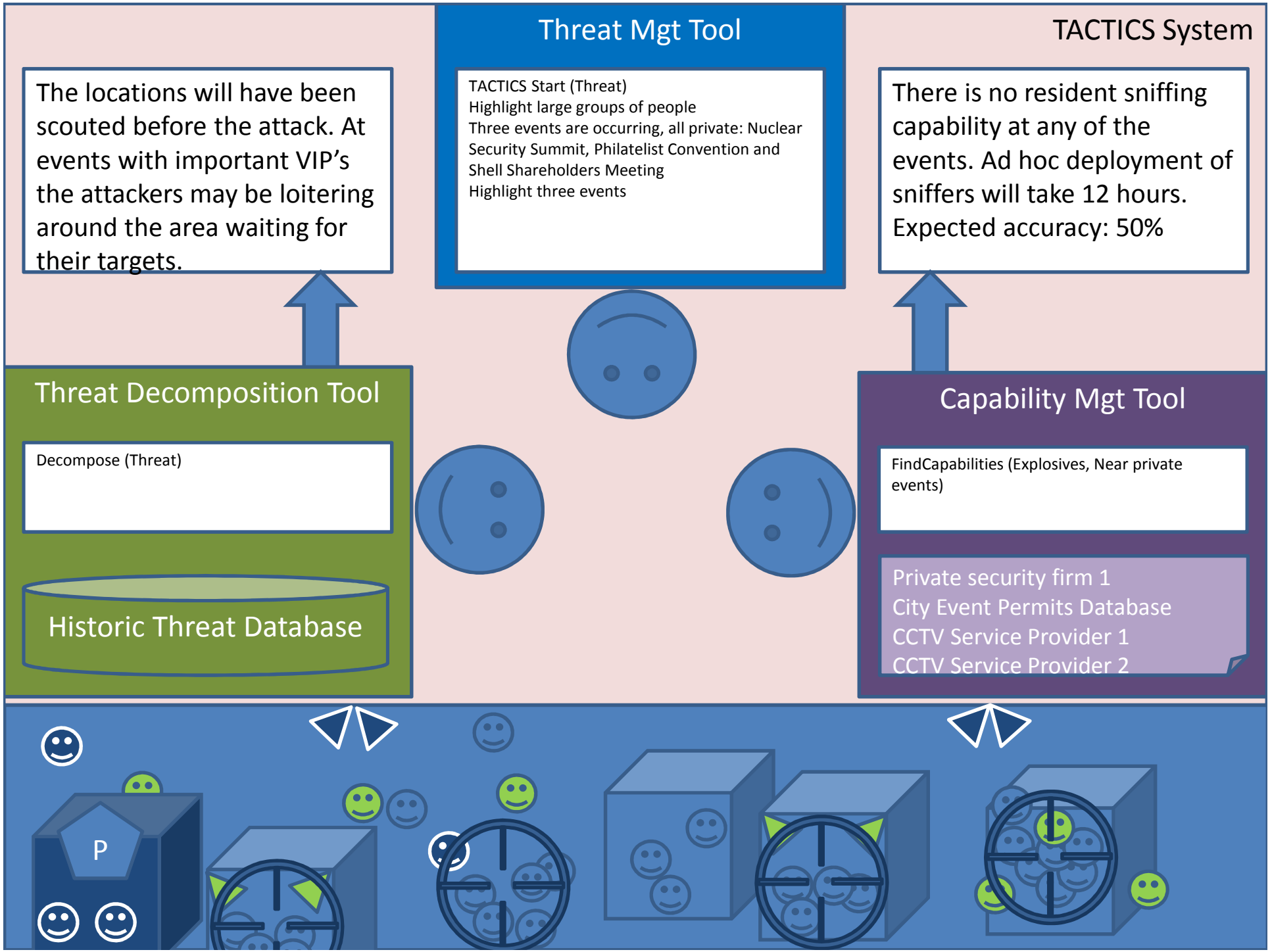

Threat Mgt Tool
TACTICS System
TACTICS Start (Threat)
Threat Decomposition Tool
Historic Threat Database
Capability Mgt Tool
Private security firm 1
City Event Permits Database
CCTV Service Provider 1
CCTV Service Provider 2
P


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


TACTICS System
Threat Mgt Tool
TACTICS Start (Threat)
Highlight large groups of people
Look for multiple terrorists; multiple targets; possible targets are large groups of people with a high symbolic profile.
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?
TACTICS Start (Threat)
Highlight large groups of people
Three events are occurring, all private: Nuclear Security Summit, Philatelist Convention and Shell Shareholders Meeting
Highlight three events
Let's focus on the explosives. Can we detect them near the private events?
Threat Decomposition Tool
Decompose (Threat)
Historic Threat Database
Capability Mgt Tool
FindCapabilities (Explosives, Near private events)
Private security firm 1
City Event Permits Database
CCTV Service Provider 1
CCTV Service Provider 2
P

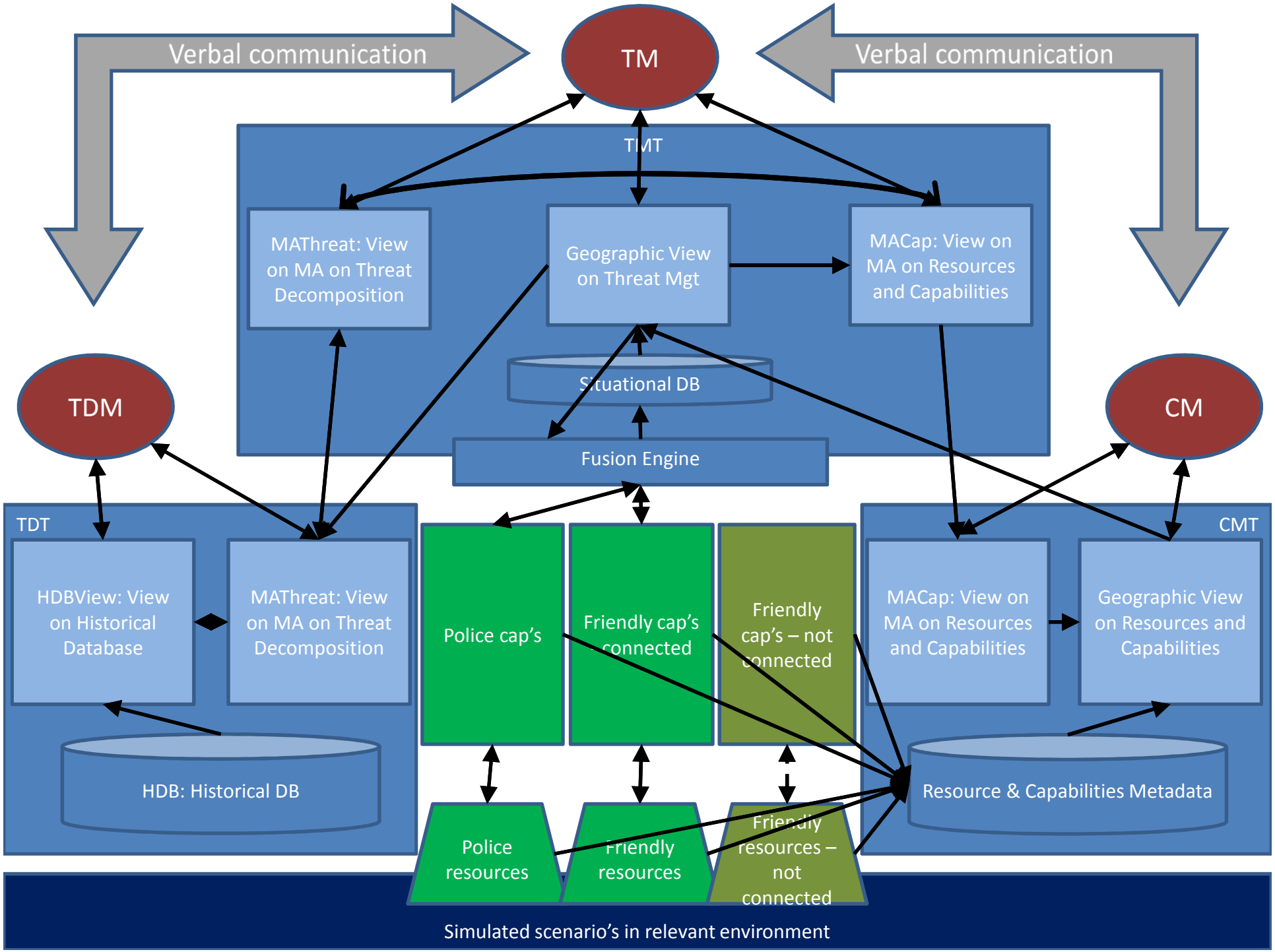

TACTICS System
Threat Mgt Tool
TACTICS Start (Threat)
Highlight large groups of people
Three events are occurring, all private: Nuclear Security Summit, Philatelist Convention and Shell Shareholders Meeting
Highlight three events
The locations will have been scouted before the attack. At events with 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
Decompose (Threat)
Historic Threat Database
Capability Mgt Tool
FindCapabilities (Explosives, Near private events)
Private security firm 1
City Event Permits Database
CCTV Service Provider 1
CCTV Service Provider 2
P

TACTICS Validation System

As described and motivated in D3.2

Legend:

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


Verbal communication
TM
Verbal communication
TMT
MAThreat: View on MA on Threat Decomposition
Geographic View on Threat Mgt
MACap: View on MA on Resources and Capabilities
Situational DB
TDM
CM
Fusion Engine
TDT
CMT
HDBView: View on Historical Database
MAThreat: View on MA on Threat Decomposition
Police cap's
Friendly cap's – connected
Friendly cap's – not connected
MACap: View on MA on Resources and Capabilities
Geographic View on Resources and Capabilities
HDB: Historical DB
Resource & Capabilities Metadata
Police resources
Friendly resources
Friendly resources – not connected
Simulated scenario's in relevant environment

TMT Modules

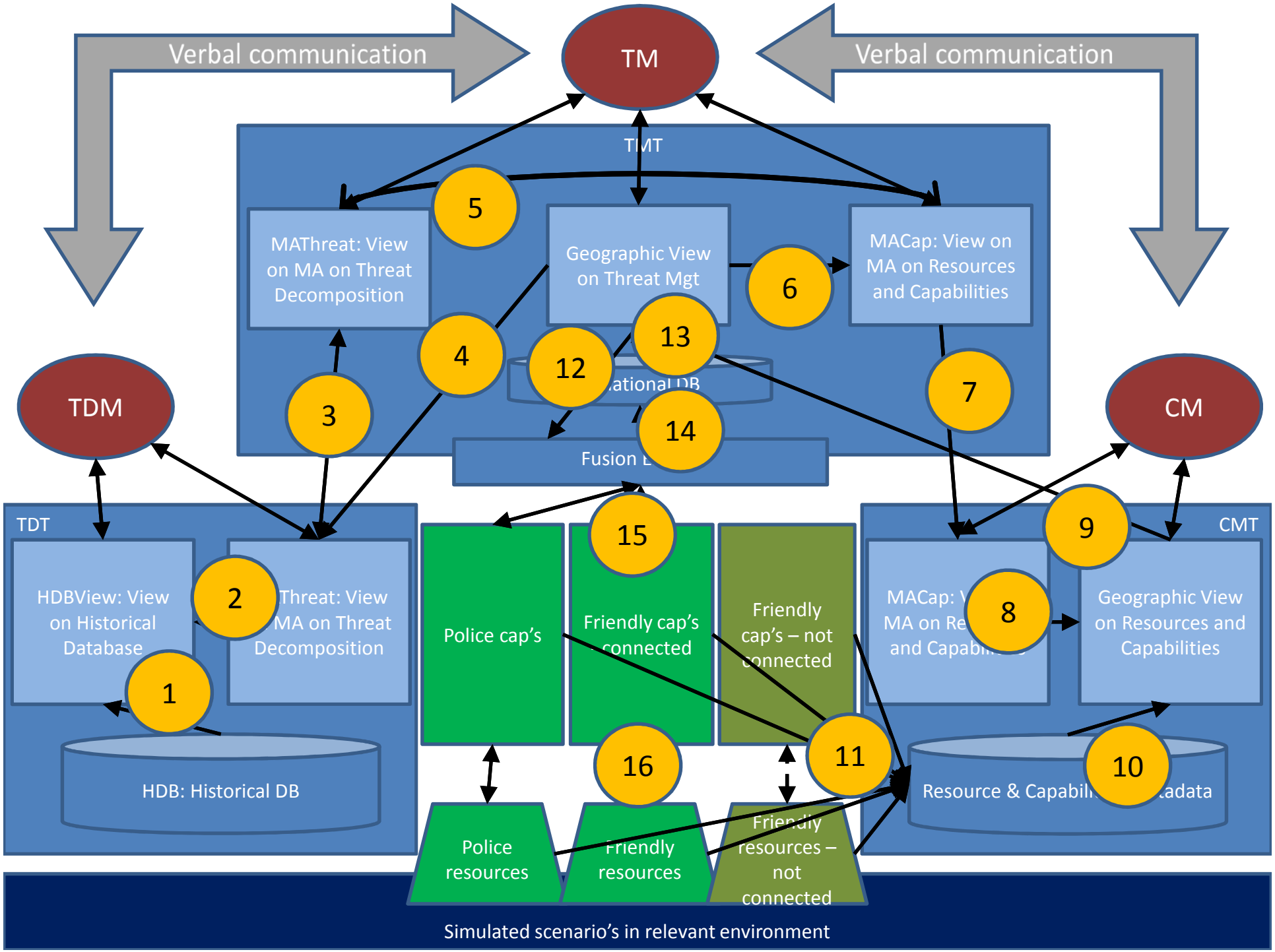
Name	Function	Detail
TMT	Give an overview of the actual situation, the threat and possible prevention or response actions	Three separate GUI's (screens)
TMT:Geo	Give situational awareness to TM	
TMT:SitDB	Store actual situation in metadata and data	Contains video, tracks, detections, etc.
TMT:Fusion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

TDT Modules

Name	Function	Detail
TDT	To support TDM to generate unbiased threat information and supply this to TM (via link to TMT)	Two separate GUI's (screens)
TDT:HDB	Store historical incident metadata	Nice to have
TDT:HDBView	Show and search historical metadata	relate to configurations
TDT:MAThreat	Described unbiased threat information	Morfological analysis view; using input from HDB and TM

CMT Modules

Name	Function	Detail
CMT	To support the CM to generate actual references to capability and resources	Two separate GUI's (screens);
CMT:Geo	Show geographic view on availability, location and QoS parameters of capabilities and resources	
CMT:MACap	Show TM requests	Morfological analysis view
CMT:RCDB	Collect and store actual resource and capability metadata	using input from both TACTICS and friendly resources and capabilities


Verbal communication
TM
Verbal communication
TMT
5
MAThreat: View on MA on Threat Decomposition
Geographic View on Threat Mgt
6
MACap: View on MA on Resources and Capabilities
4
12
13
7
TDM
3
14
CM
Fusion D
TDT
15
9
CMT
HDBView: View on Historical Database
2
Threat: View MA on Threat Decomposition
Police cap's
Friendly cap's connected
Friendly cap's – not connected
MACap: V MA on Re and Capabi
8
Geographic View on Resources and Capabilities
1
11
16
10
HDB: Historical DB
Resource & Capabili adata
Police resources
Friendly resources
Friendly resources – not connected
Simulated scenario's in relevant environment

Id	Sender	Receiver	Information	Datatype
1	TDT:HDB	TDT:HDBView	Descriptions of historical incidents	texts / keywords
2	TDT: HDBView	TDT:MAThreat	Links between (partial) configurations and historical incidents	Keywords + partial configurations
3	TDT:MAThreat	TMT:MAThreat	Decomposed threat information	(partial) configurations
3	TMT:MAThreat	TDT:MAThreat	Suggestions to decompose	(partial) configurations
4	TMT:Geo	TDT:MAThreat	More detailed threat information	Free text (for logging)
5	TMT:MAThreat	TMT:MACap	Threats to find capabilities for	(partial) configurations
5	TMT:MACap	TMT:MAThreat	Capabilities to address threats	(partial) configurati
6	TMT:Geo	TMT:MACap	Area selection for capabilities	Area
7	TMT:MACap	CMT:MACap	Request for capabilities, including area	(partial) configurations + area
8	CMT:MACap	CMT:Geo	Request for capabilities, including area	(partial configurations + area)
9	CMT:Geo	TMT:Geo	Ranked list of available capabilities and resources	List of capabilities + resources (URL, configuration)

No technical link from MA to Geographical View

Id	Sender	Receiver	Information	Datatype
10	CMT:CapDB	CMT:Geo	Resource and capability metadata	Keywords + partial configurations
11	TMT:Fusion / Resources	CMT:CapDB	Dynamic metadata per resource / capability (availability, location)	ONVIF? SensorWebEnablement?
12	TMT:Geo	TMT:Fusion	Data request / configuration based on suggestions from CMT	(Capability, resources, area, parameters)
13	TMT:SitDB	TMT:Geo	View on actual situational awareness according to TM wishes	Situational awareness
14	TMT:Fusion	TMT:SitDB	Situation updates (tracks, recognition, detection of behaviour)	Object metadata
15	Capabilities	TMT:Fusion	Fusion	Object metadata
15	TMT:Fusion	Capabilities	Data requests / configuration updates	(Capability, resources, area, parameters)
16	Capabilities	Resources	Data requests / configuration updates	(Resources, area, parameters)
16	Resources	Capabilities	Raw data	Video / audio / text / …