Analytics for detecting deviant behaviour in TACTICS

TACTICS@IFSEC

Jeroen van Rest, MSc., TNO

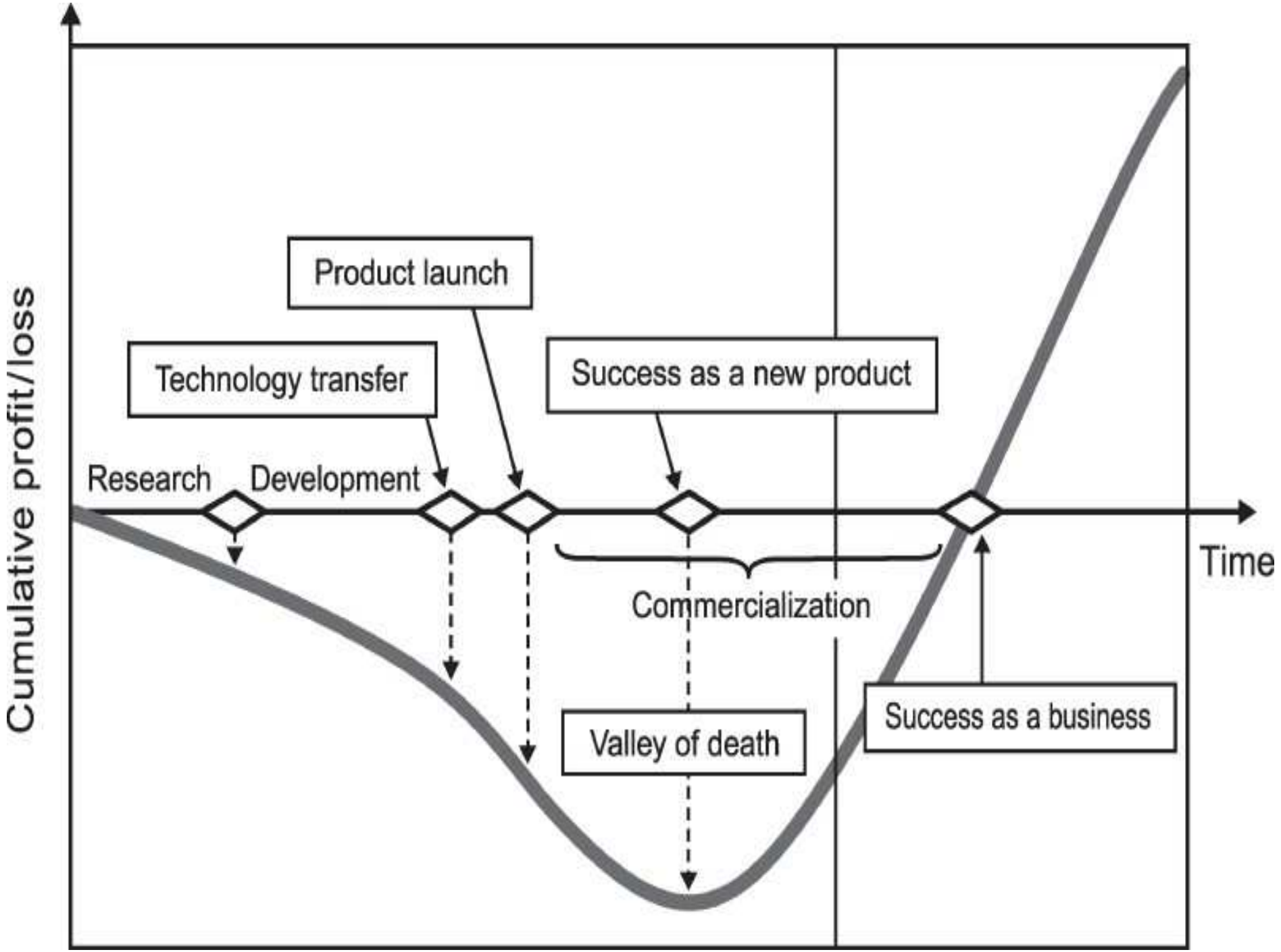
London

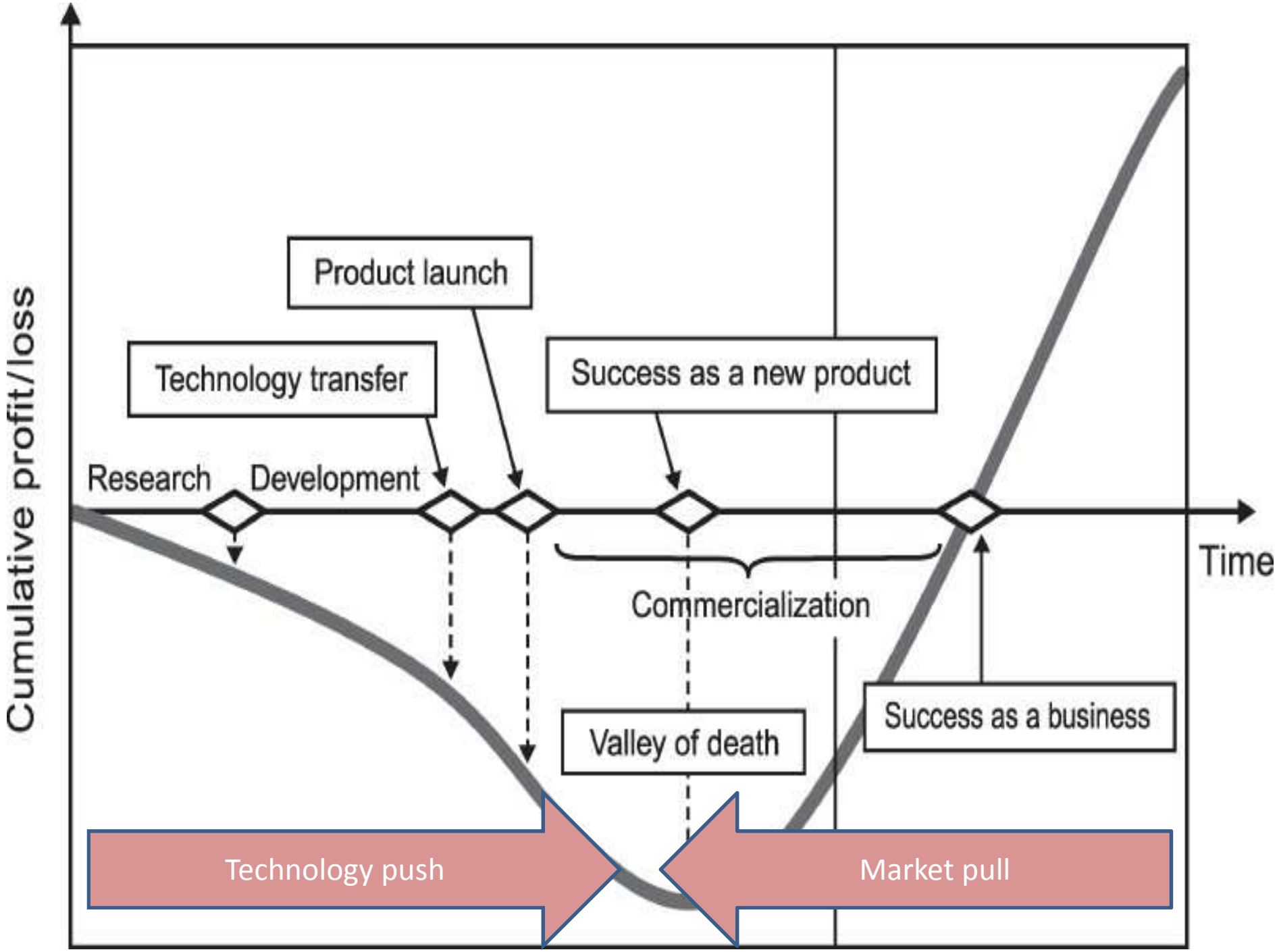
June 19th 2014

 Grant Agreement no. 285533

Outline

- Part 1: Technology Push of Proactive Video Analytics
- Part 2: Market Pull of Detection of Deviant Behaviour
- Part 3: Tactical Approach to Counter Terrorists in Cities (TACTICS)


Cumulative profit/loss
Product launch
Technology transfer
Success as a new product
Research
Development
Time
Commercialization
Valley of death
Success as a business

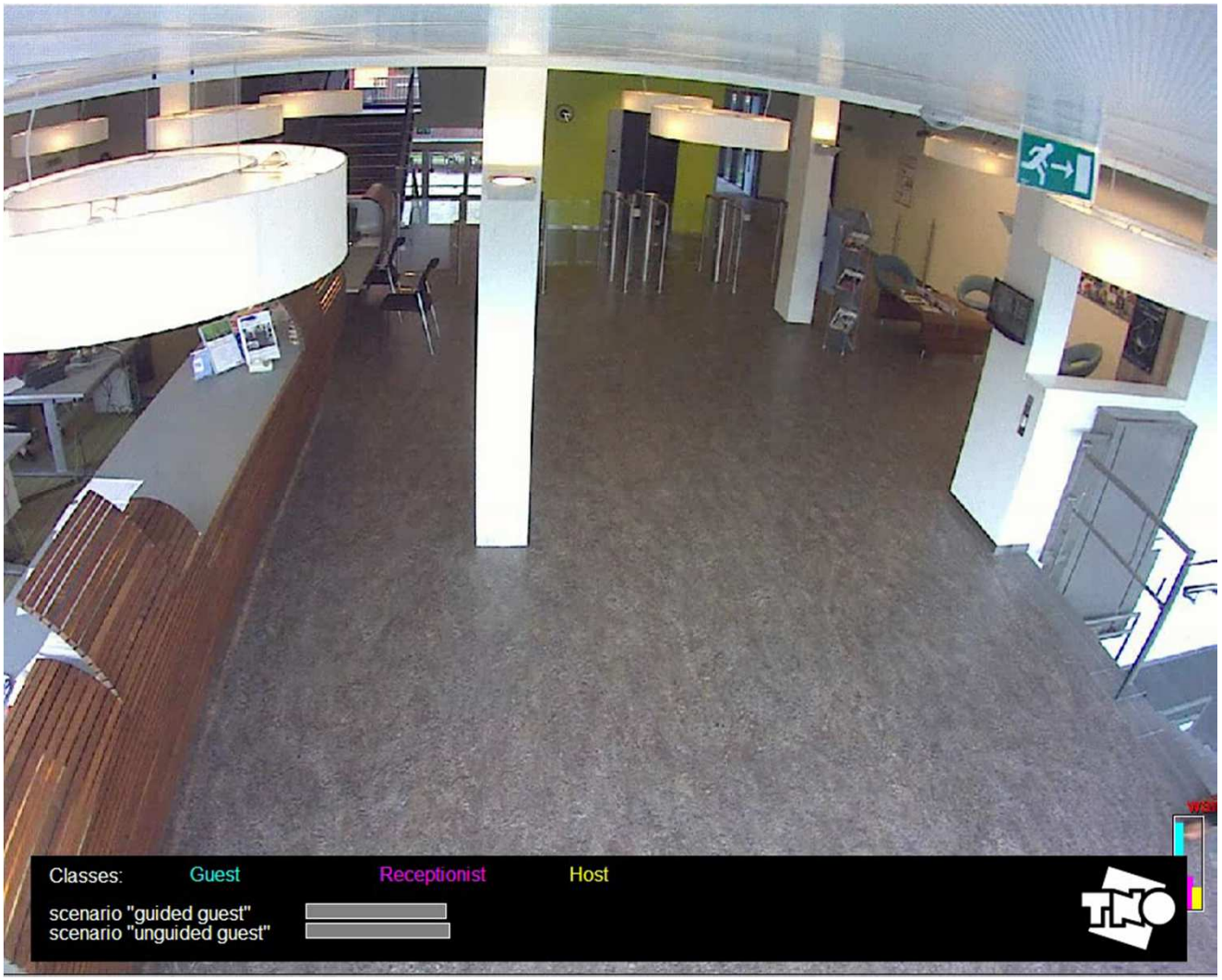

Cumulative profit/loss
Product launch
Technology transfer
Success as a new product
Research
Development
Time
Commercialization
Valley of death
Success as a business
Technology push
Market pull

Outline

- **Part 1: Technology Push of Proactive Video Analytics**
- Part 2: Market Pull of Detection of Deviant Behaviour
- Part 3: Tactical Approach to Counter Terrorists in Cities (TACTICS)

Behaviour is a constellation of actions and reactions

Behaviour is a constellation of actions and reactions

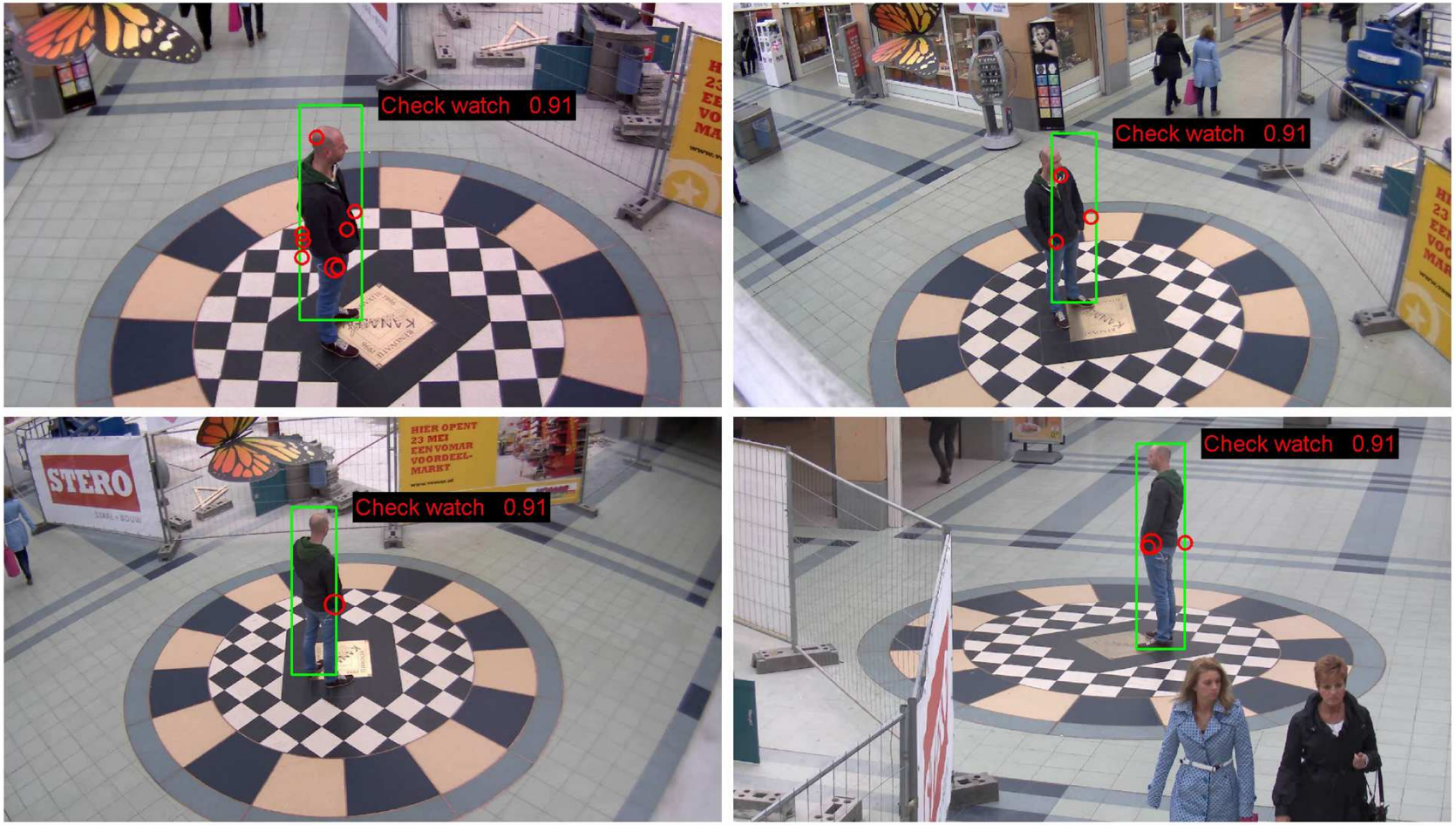


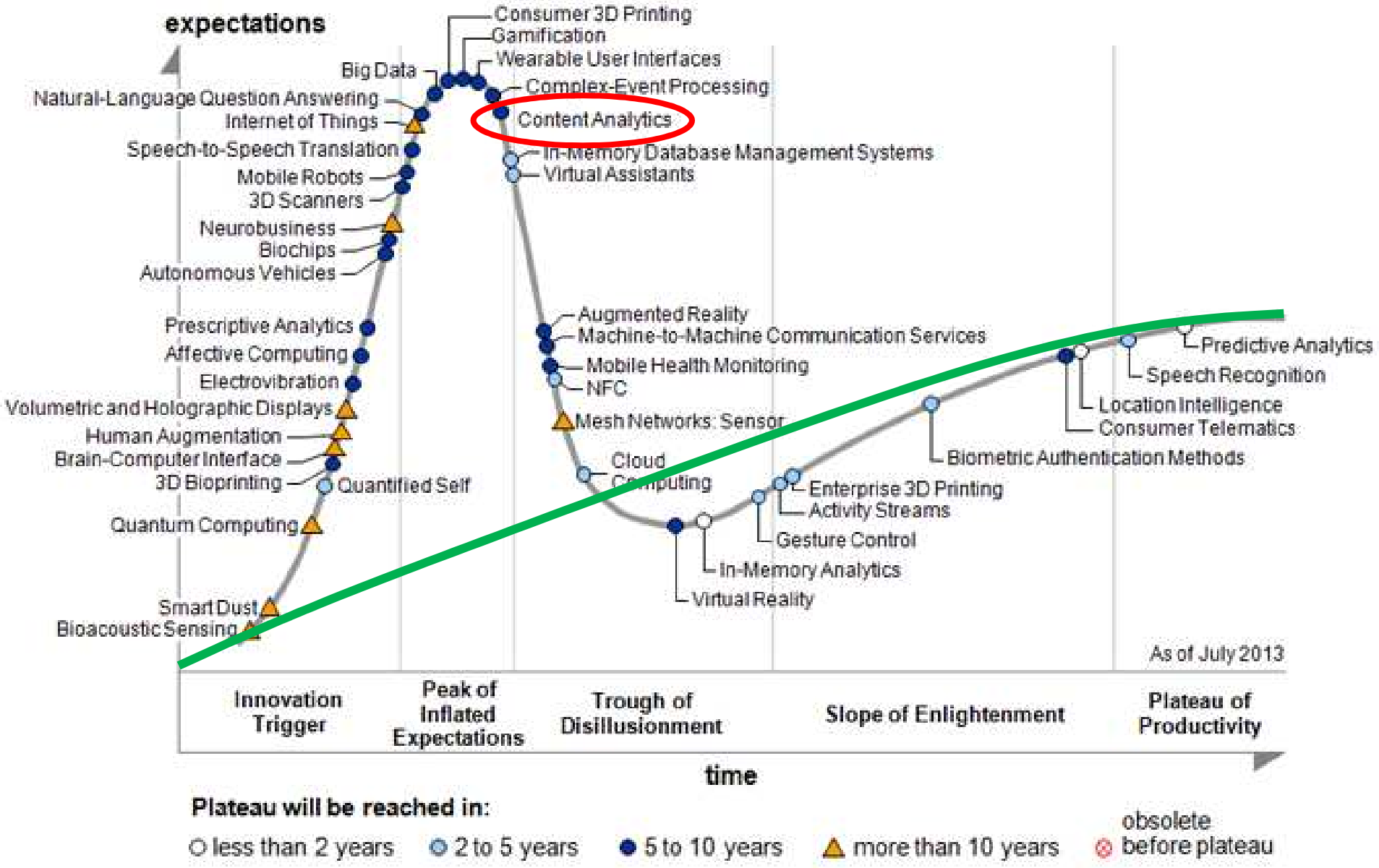
~10% improvement per additional viewpoint (tracking)

~10% improvement per additional viewpoint (tracking)

~10% improvement per additional viewpoint (actions)

~10% improvement per additional viewpoint (actions)





Hype cycle for Emerging Technologies 2013; Source: Gartner August 2013

Mature content analytics

Examples:

- Intrusion detection
- Identification in controlled situations (ANPR and Biometrics)
- People counting
- Loitering

➔ Simple, small scenes.

Technological developments

- Limited coverage ➔ Continuous multi-viewpoint omnidirectional coverage
- Fixed ➔ Moving camera platforms
- Single person ➔ Crowded scenes
- Optimal lighting ➔ Poor lighting
- Single modality ➔ Fusion of multiple modalities

Allowing for:

(1) Surveillance on free flow of people, and therefor in one sense less invasive surveillance;

(2) Early detection of weak signals;

Technological developments

- Limited coverage ➔ Continuous multi-viewpoint omnidirectional coverage
- Fixed ➔ Moving camera platforms
- Single person ➔ Crowded scenes
- Optimal lighting ➔ Poor lighting
- Single modality ➔ Fusion of multiple modalities

Allowing for:

(1) Surveillance on free flow of people, and therefor in one sense **less invasive** surveillance;

(2) Early detection of weak signals;

Mitigating threats in crowded situations

- Aggression, shoplifting, pickpocketing, left luggage, swindling and drug dealing;

- Organised crime or even terrorism;

➔ complex, dynamic scenes: interaction between people is key for understanding the scene

Effective video analytics for deviant behaviour

1. **Garbage-in is garbage-out**: camera coverage, viewpoints, quality of cameras and network. You cannot fix something that is fundamentally broken.
2. The performance of video analytics improves with **~10% per additional viewpoint** on the scene, if the relative positions of cameras are accurately known.
3. **Behaviour is a constellation of actions and reactions**. A single action in a complex environment says nothing and only leads to false alarms. Therefor, tracking and recognition are essential. Identification however is too much detail and introduces unnecessary privacy risks.
4. **Test data** is needed. Because of privacy concerns few and old sets are publicly available. We have built a video database of pickpockets: 30 incidents amidst normal shopping behaviour. You are invited to join this effort.
5. **This kind of technology potentially increases specific biases**. Privacy by Design is still in its infancy, both as a policy instrument, and as a technical tool. We develop Privacy Enhancing Technologies such as dynamic masking and encrypted metadata databases to actively detect and mitigate biases and privacy risks.
6. A **technology roadmap** to introduce this kind of technology in your organisation should address policies, work processes, user interfaces, analytics and ICT infrastructure.

Dataset of 30 pickpocket incidents in shopping mall

- Validated by Dutch National Police, Royal Marechaussee and shopping mall security staff
- High quality video recordings
- Different modi operandi of collaborating pickpockets
- Amidst normal shopping behaviour

Bouma, H. et al, *Automatic detection of suspicious behavior of pickpockets with track-based features in a shopping mall* in SPIE Optics and Photonics for Counterterrorism, Crime Fighting and Defence, accepted for submission

Outline

- Part 1: Technology Push of Proactive Video Analytics
- **Part 2: Market Pull of Detection of Deviant Behaviour**
- Part 3: Tactical Approach to Counter Terrorists in Cities (TACTICS)

- WICLEIM2014 Rob de Wijk
- Operations Dutch Police

Criminal phases

- Broad target selection
- Intelligence and surveillance
- Specific target selection
- Pre-attack surveillance & planning
- Attack rehearsal
- Execution: actions on objective
- Escape & exploitation

United States. Army Training and Doctrine Command. *A military guide to terrorism in the twenty-first century*. Cosimo Incorporated, 2010.

Criminal phases

- Creating motivation
- Broad target selection
- Intelligence and surveillance
- Specific target selection
- Pre-attack surveillance & planning
- Attack rehearsal
- Execution: actions on objective
- Escape
- Exploitation
- Repent
- Rehabilitation

Criminal phases

- **Creating motivation**
- **Broad target selection**
- **Intelligence and surveillance**
- **Specific target selection**
- **Pre-attack surveillance & planning**
- **Attack rehearsal**
- **Execution: actions on objective**
- Escape
- Exploitation
- Repent
- Rehabilitation

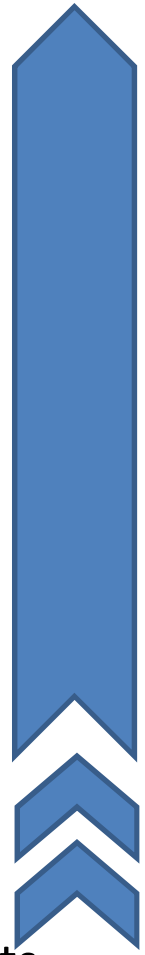
Proactive security

Effectiveness of proactive security

Security processes / Criminal phases	Preparation	Prevention	Intelligence	Disturb	In the act	Investigate	Recover
Create motivation							
Broad target selection							
Intelligence and surveillance							
Specific target selection							
Pre-attack surveillance & planning							
Attack rehearsal							
Execution							
Escape							
Exploitation							
Repent							
Rehabilitation							

Threat mitigation

- Preparation (de-radicalisation, intelligence, testing, red-teaming, exercises);
- Prevention (prediction, nudging, “show the force”);
- Caught in the act (detection, recognition);
- Crisis response (live monitoring);
- Investigative (forensics, identification);
- Acceptance (liability);



Later in the incident ➔ increasing costs

Effectiveness of proactive security

Security processes / Criminal phases	Preparation	Prevention	Intelligence	Disturb	In the act	Investigate	Recover
Create motivation							
Broad target selection							
Intelligence and surveillance							
Specific target selection							
Pre-attack surveillance & planning							
Attack rehearsal							
Execution							
Escape							
Exploitation							
Repent							
Rehabilitation							

Example: effectiveness of CCTV

"*Displacement has long been the Achilles heel of situational measures, and CCTV is no exception*" – Gill, 2005

Effectiveness of CCTV

Security processes / Criminal phases	Preparation	Prevention	Intelligence	Disturb	In the act	Investigate	Recover
Create motivation							
Broad target selection	C	C	C	C			
Intelligence and surveillance	C	C	C	C		C	
Specific target selection	C	C	C	C		C	
Pre-attack surveillance & planning	C	C	C	C		C	
Attack rehearsal	C	C	C	C		C	
Execution	C			C	C	C	
Escape	C				C	C	
Exploitation							
Repent							
Rehabilitation	C						C

Predictive behaviour profiling

- Not based on ethnicity, age, gender, origin
- Based on behaviour
- Before the incident

“Deviant behaviour”

- Profiles of **situations and social scenario’s** based on historical data, and / or …

… based on expert knowledge.

Nine definitions of deviant behaviour (1-4): threat based

- Behaviour which may lead to dangerous and/ or undesired situations, i.e. which threaten the continuity of the processes at the location;
- Behaviour which correlates significantly with incidents;
- Behaviour which is part of the modus operandi of a criminal act;
- Behaviour which has as purpose to gain an advantage for one self at the cost of someone else: unethical behaviour;

Nine definitions of deviant behaviour (5-9): continuity based

- Behaviour which is not part of any of the allowed (work-)processes which occur at the respective location or object;
- A reaction which does not fit to the stimulus if the intent of the subject were benign;
- Behaviour which falls outside the normal distribution of behaviour at the respective location;
- Behaviour which is unwillingly displayed due to high cognitive pressure;
- Behaviour which does not fit the local social norms, including anti-social behaviour and culturally abnormal behaviour.

Outline

- Part 1: Technology Push of Proactive Video Analytics
- Part 2: Market Pull of Detection of Deviant Behaviour
- **Part 3: Tactical Approach to Counter Terrorists in Cities (TACTICS)**

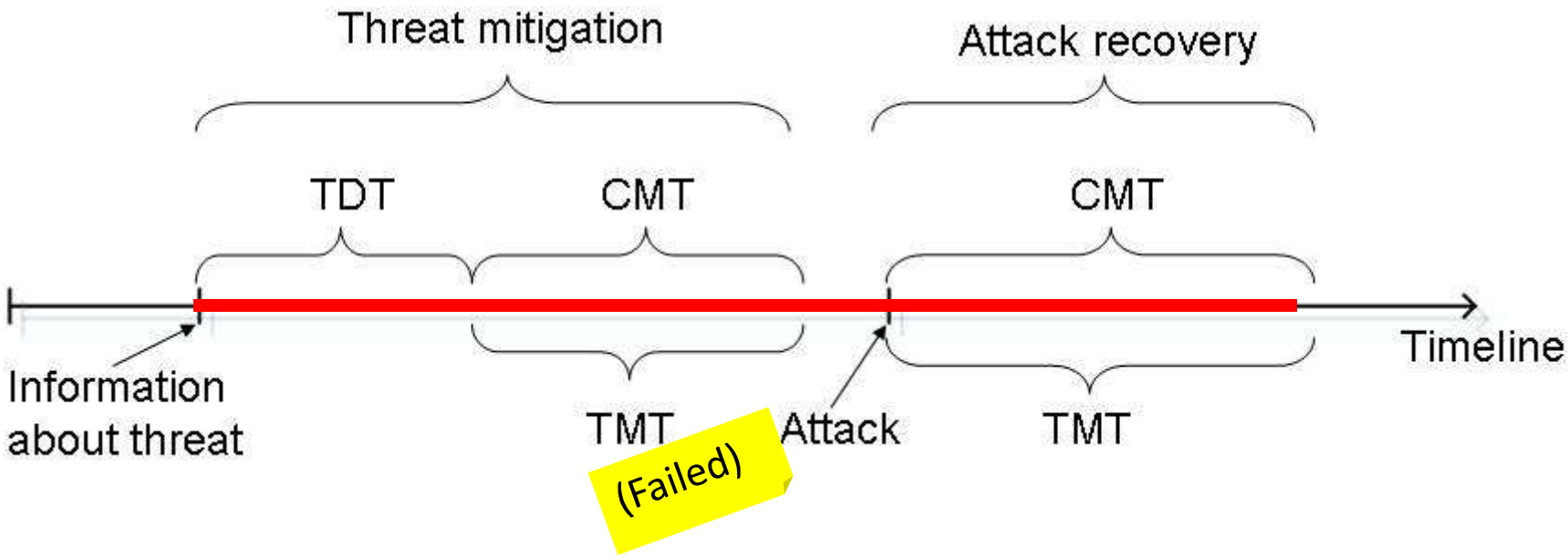
TACTICAL APPROACH TO
COUNTER TERRORISTS IN CITIES

September 2012 – August 2014

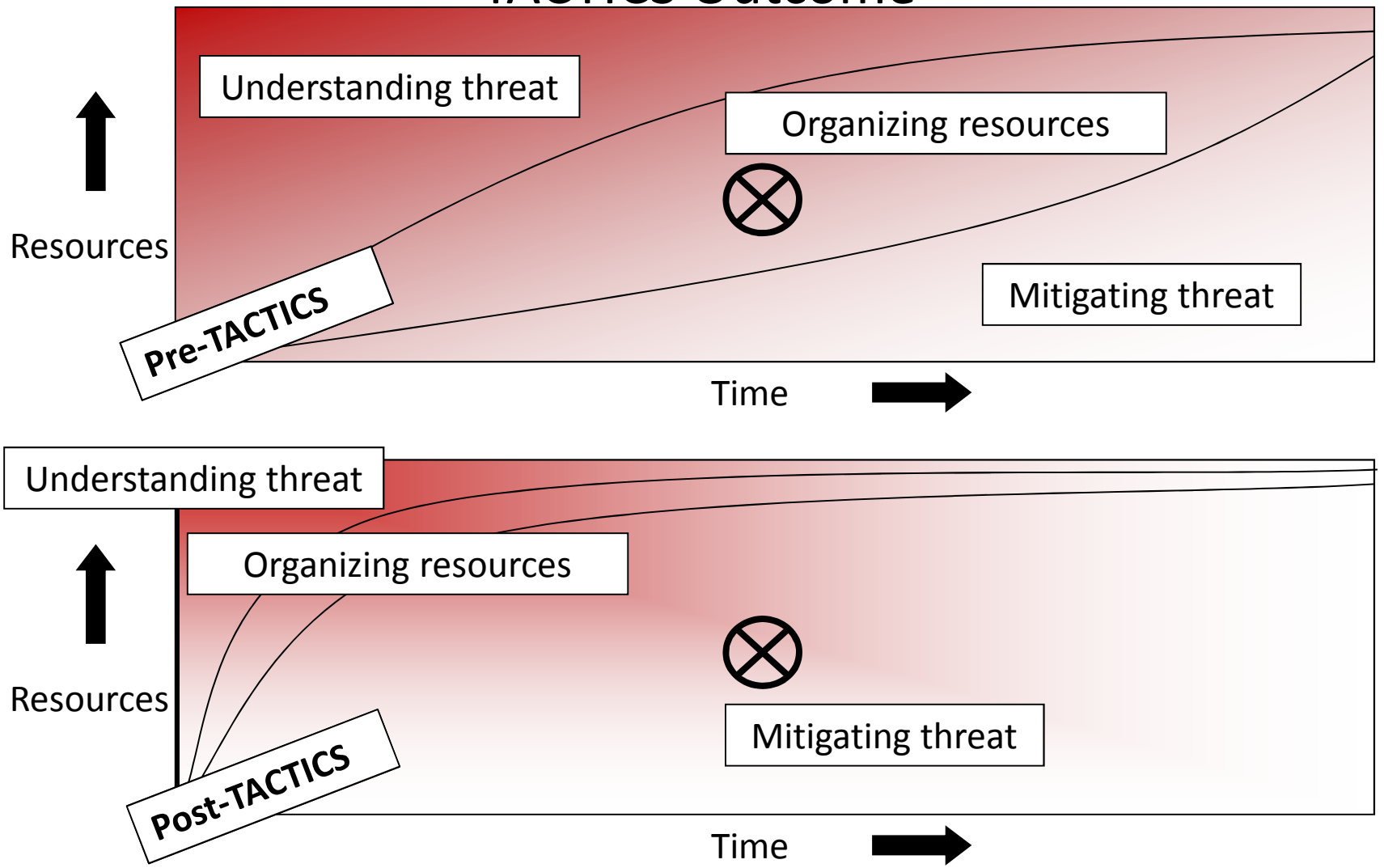
TACTICS Abstract

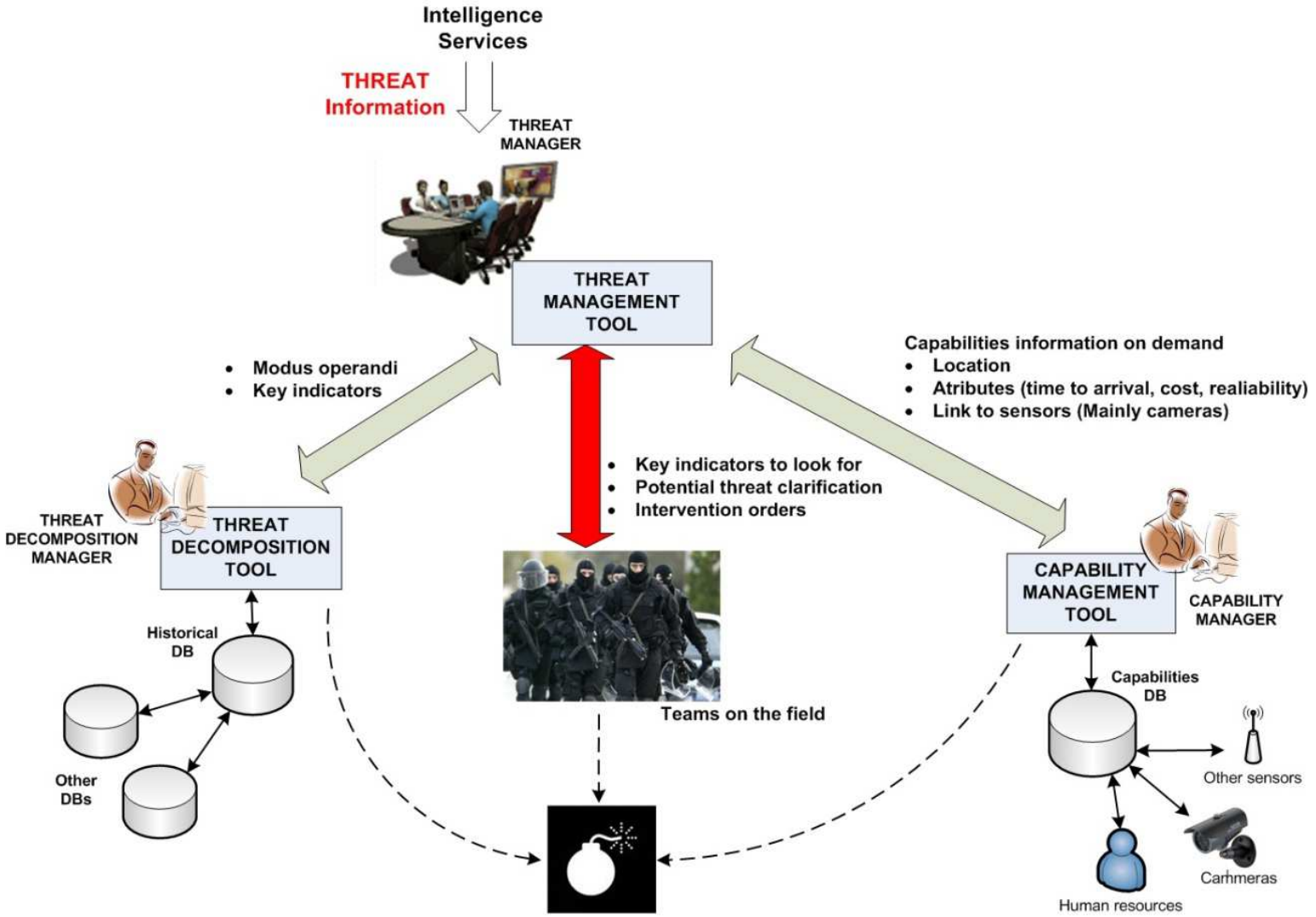
TACTICS seamlessly integrates new research results in the area of **behaviour analysis**, **characteristics of the possible urban-based targets** and **scenario awareness** into a **decision making framework** comprising of **a coherent set of tools and related processes**, supporting security forces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

Temporal Decomposition (and scope of TACTICS)



TACTICS Outcome



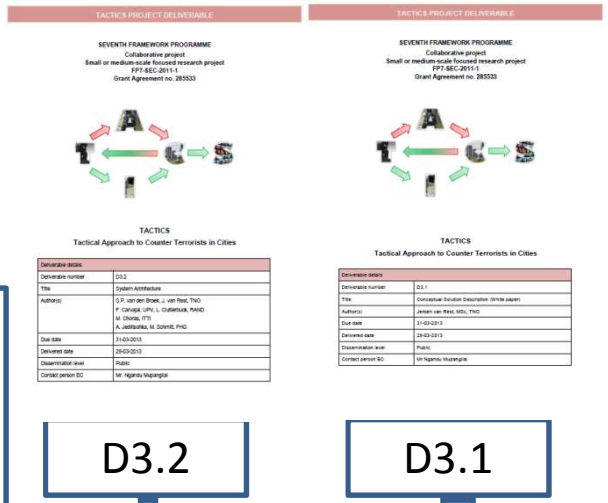

Intelligence Services
THREAT Information
THREAT MANAGER
THREAT MANAGEMENT TOOL
Modus operandi
Key indicators
Capabilities information on demand
Location
Atributes (time to arrival, cost, realiability)
Link to sensors (Mainly cameras)
Key indicators to look for
Potential threat clarification
Intervention orders
THREAT DECOMPOSITION MANAGER
THREAT DECOMPOSITION TOOL
Historical DB
Other DBs
Teams on the field
CAPABILITY MANAGEMENT TOOL
CAPABILITY MANAGER
Capabilities DB
Other sensors
Carhmeras
Human resources

TACTICS System Engineering View

TACTICS is a research project which uses software to validate some of the hypotheses. This requires both a scientific and a system engineering view on TACTICS.

Engineering view: at least three design phases:

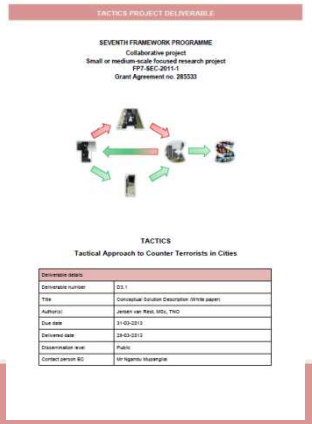
1. Proposal phase:
   - Goal: Write a winning proposal;
   - Result: TACTICS project proposal (“paper system”)
2. TACTICS Project phase:
   - Goal: Research and validation
   - Result:
     1. Reports (most deliverables)
     2. Validation system (software and manuals)
3. Operational integration phase:
   - Goal: Create an operational product
   - Result: operational product(s)



WP3 Results overview: D3.1

D3.1: White paper with the conceptual framework including interoperability with the systems context: "*Conceptual Solution Description*"

- Glossary (*Deviant behaviour*, *Profiling*, *Design Patterns*, …);
- Design Principles (*Scoping*, *User Centred Design*, *Ethics & Privacy by Design, Design Processes);*
- Conceptual Solution Description (*Threat Decomposition*, *Capability Management* and *Threat Management*)
- Data model requirements (*9 Surveillance Requirements*, *collection for investigation phase*, …)


TACTICS PROJECT DELIVERABLE

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

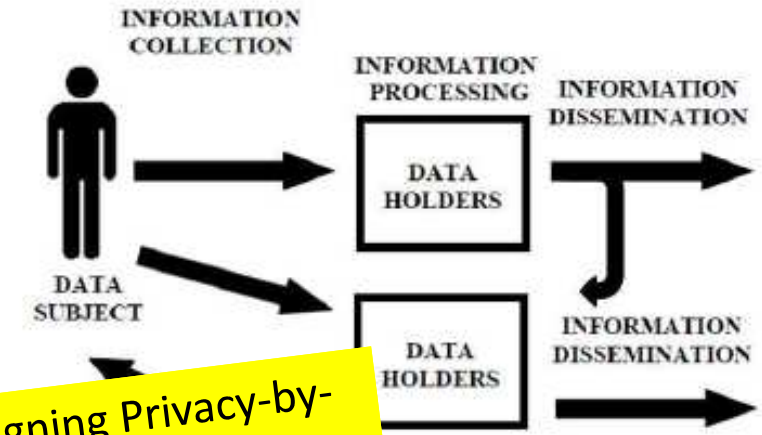
TACTICS
Tactical Approach to Counter Terrorists in Cities

Deliverable details	
Deliverable number	D3.1
Title	Conceptual Solution Description (White paper)
Author(s)	Jeroen van Rest, MDU, TNO
Due date	31-03-2013
Delivered date	28-03-2013
Dissemination level	Public
Contact person SC	Mr Ngambu Mulenga

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.

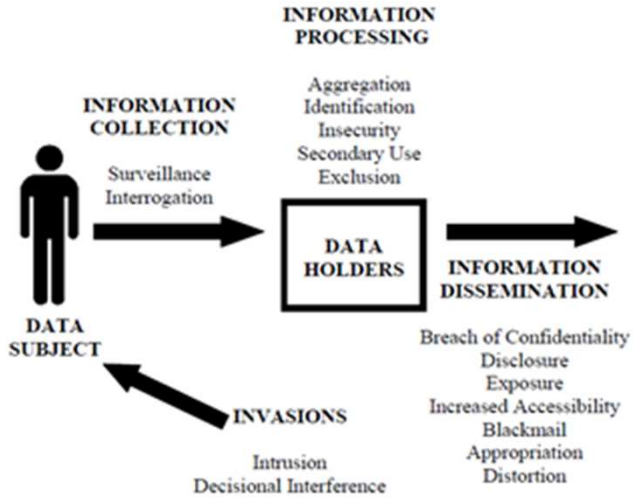
- Follow the law
- (Re)designing Privacy by Design
- Identifying privacy invading activities
- Specifying 7 + 1 principles of PbD
- Methodological approach



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

Invasiveness

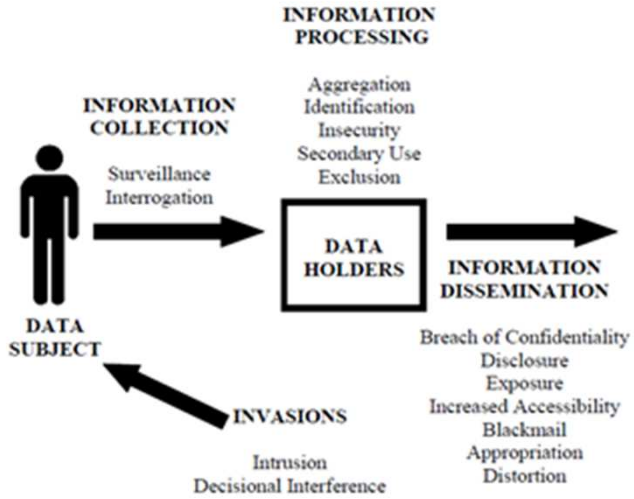
- Surrender of autonomy / cooperation
- Level of detail of personal data
- “Bycatch” of personal data (camera versus personal tracking device)
- More than legally allowed (espionage is more invasive than surveillance)
- Different from communicated publicly (e.g. covert surveillance)



Solove, A taxonomy of privacy, 2006

Invasiveness

- **Surrender of autonomy / cooperation**
- **Level of detail of personal data**
- “Bycatch” 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

Invasiveness

Invasiveness				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

Methodological approach to specifying deviant 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
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						

(Early draft)

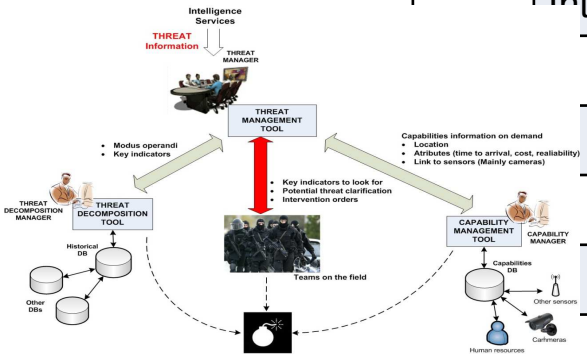
Morphological analysis

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



TACTICS Beyond State of the Art (1/2)

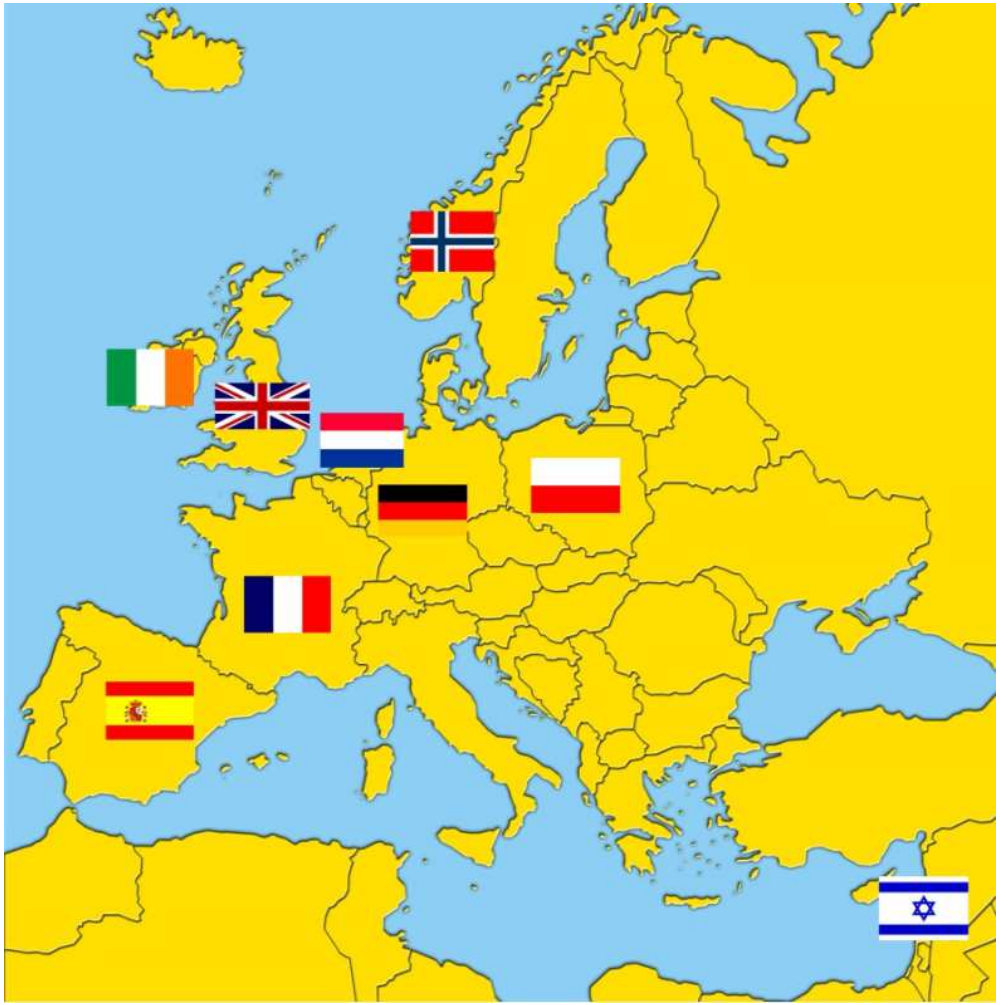
State of the Art	Beyond state of the art
Defining deviant behaviour by asking security personnel what is deviant through their eyes.	• Defining deviant behaviour by decomposing threats into past and future modus operandi and deviant behaviour • Defining specific deviant behaviour by coupling characteristics 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)

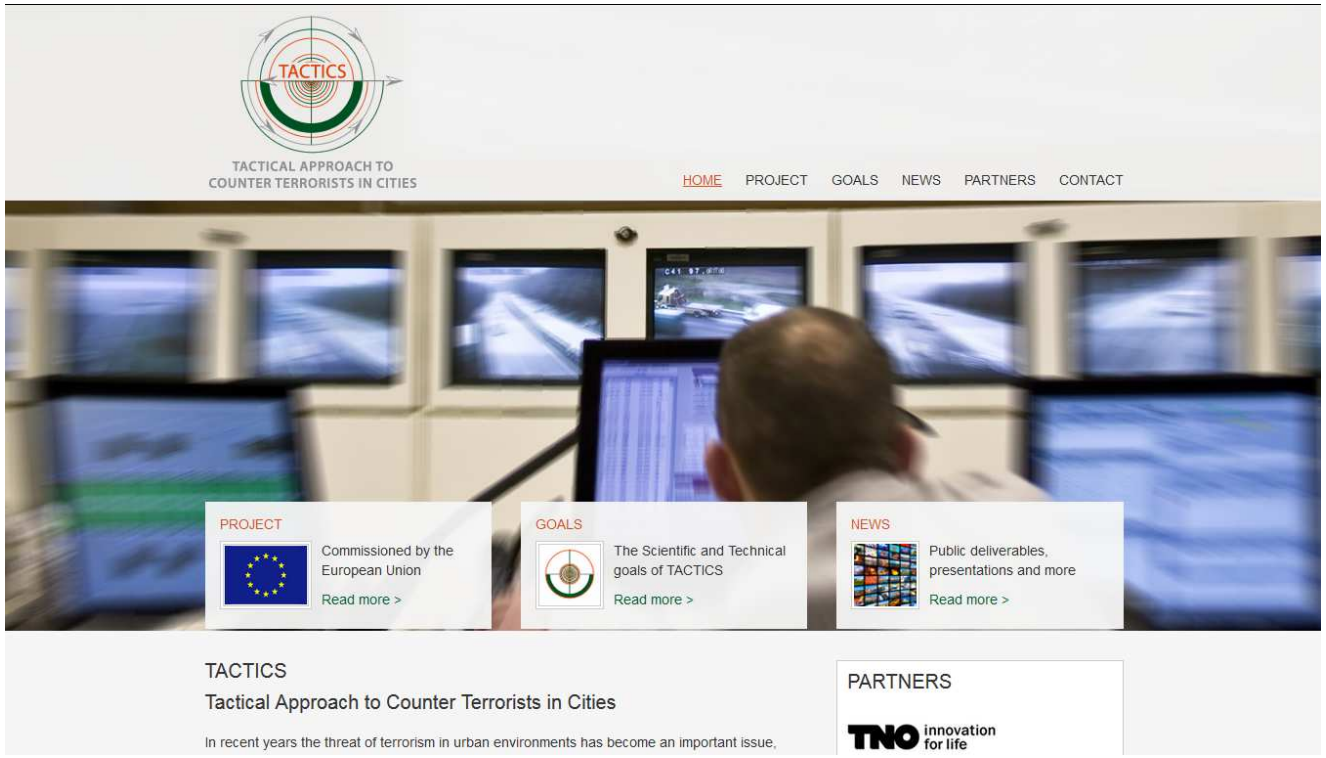
State of the Art	Beyond state of the art
Adding extra personnel and physical sensors to get surveillance capabilities that are normally not present	• Re-using existing personnel and sensors for surveillance capabilities that are normally not present
Communication and decision about a threat or attack 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.

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!



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

Surveillance requirements on Metadata

1. Coverage of relevant domain
2. Metadata about the sensor
3. Metadata about features/observations
4. Metadata about entities, events, actions and their attributes.
5. Metadata about situations and scenarios (relations between observables)
6. Describe goals, hypothetical situations and scenarios
7. Traceability
8. Uncertainty and alternatives
9. Observation capabilities

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)

References

Selected papers

- 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.
- Sanromà, Gerard, Gertjan Burghouts, and Klamer Schutte. "Recognition of long-term behaviors by parsing sequences of short-term actions with a stochastic regular grammar." *Structural, Syntactic, and Statistical Pattern Recognition*. Springer Berlin Heidelberg, 2012. 225-233.
- 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.
- Bouma, Henri, et al. "Recognition and localization of relevant human behavior in videos." 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, G. J., et al. "Selection of negative samples and two-stage combination of multiple features for action detection in thousands of videos." Machine Vision and Applications 25.1 (2014): 85-98.
- Bouma, Henri, et al. "WPSS: Watching people security services." *SPIE Security+ Defence*. International Society for Optics and Photonics, 2013.
- Bouma, Henri, et al. "Re-identification of persons in multi-camera surveillance under varying viewpoints and illumination." *SPIE Defense, Security, and Sensing*. International Society for Optics and Photonics, 2012.
- Rest, J., et al. "Sensors and tracking crossing borders." *In Proceedings of the 4th Conference on Safety and Security Systems in Europe*. 2009.
- van Rest, Jeroen, et al. "Designing Privacy-by-Design." *Privacy Technologies and Policy*. Springer Berlin Heidelberg, 2014. 55-72.
- 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.
- Lefter, I., L. J. M. Rothkrantz, and G. J. Burghouts. "A comparative study on automatic audio–visual fusion for aggression detection using meta-information." *Pattern Recognition Letters* 34.15 (2013): 1953-1963.
- Andersson, Maria, et al. "Activity recognition and localization on a truck parking lot." *Advanced Video and Signal Based Surveillance (AVSS), 2013 10th IEEE International Conference on*. IEEE, 2013.
- Bouma, Henri, et al. "Behavioral profiling in CCTV cameras by combining multiple subtle suspicious observations of different surveillance operators." *SPIE Defense, Security, and Sensing*. International Society for Optics and Photonics, 2013.
- van Rest, J., et al. "Requirements for multimedia metadata schemes in surveillance applications for security." *Multimedia Tools and Applications* (2013): 1-26.
- Bouma, H. et al, (2014) Integrated roadmap towards fast finding and tracking people at large airports (*in review)*
- Rest, et al (2014) *Deviant Behaviour*, TNO Report (in re view)

Selected patents

- System and method for identifying image locations showing the same person in different images
- US2013163819 (A1) - SYSTEM AND METHOD FOR INDENTIFYING IMAGE LOCATIONS SHOWING THE SAME PERSON IN DIFFERENT IMAGES