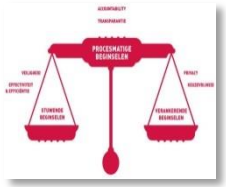
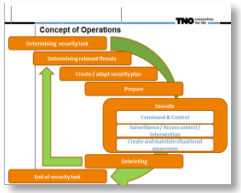
Deviant Behaviour

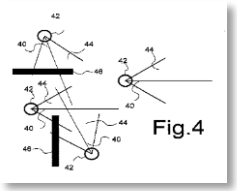
Jeroen van Rest

April 2nd 2014, ASIS Europe, The Hague

Outline

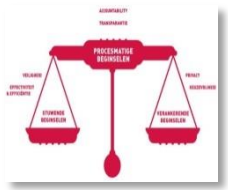




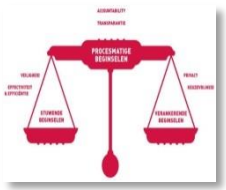


- Why deviant behaviour?
- How to use deviant behaviour?
- What to do to use deviant behaviour?

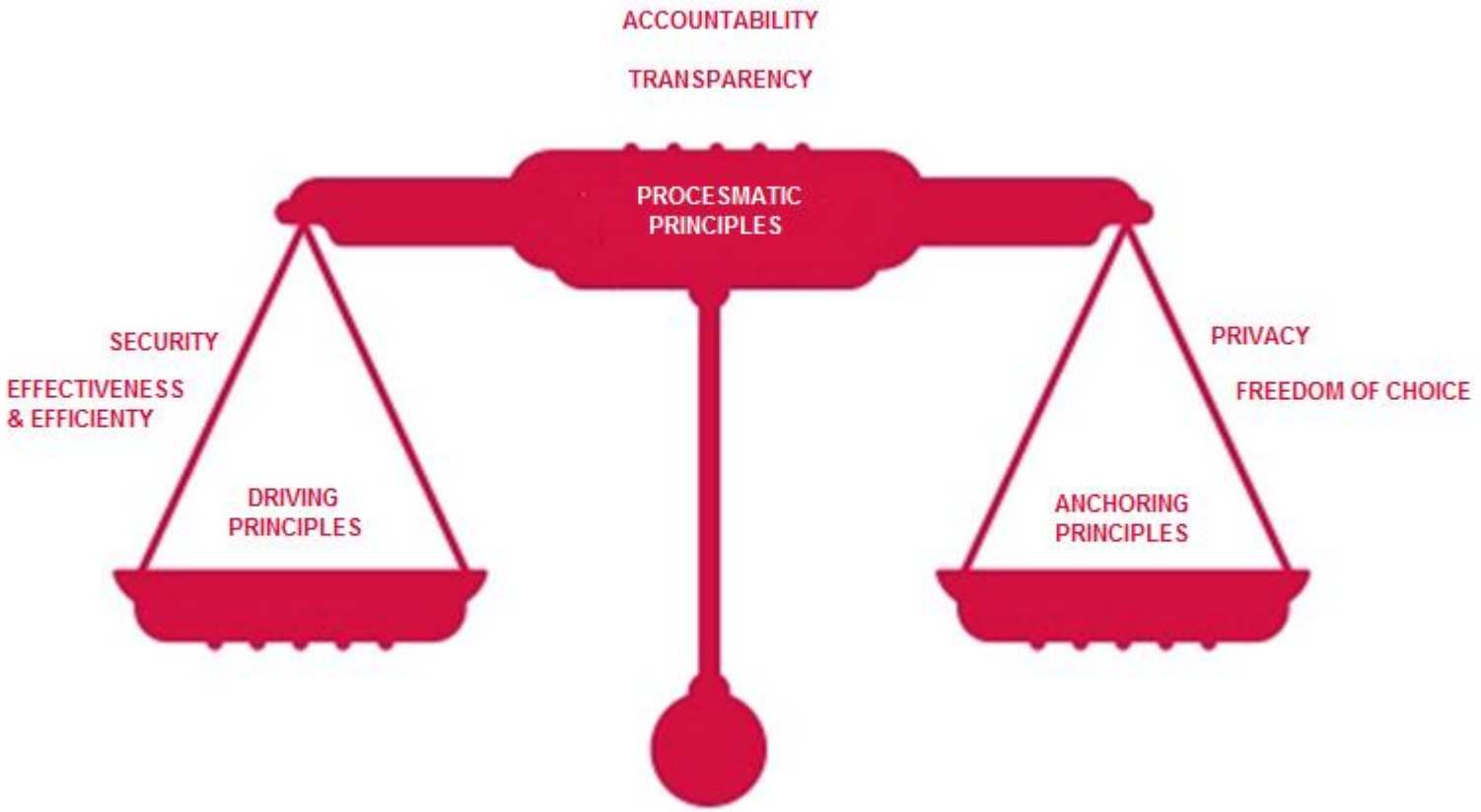
- Sources
- Recap
- Recommendation



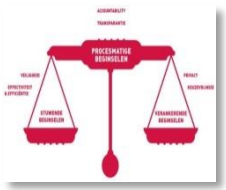
Why deviant behaviour?



Why deviant behaviour?



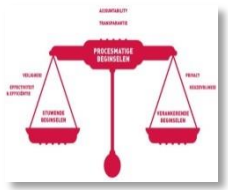
iOverheid (*iGovernment*) - http://www.ioverheid.nu/



Why deviant behaviour?

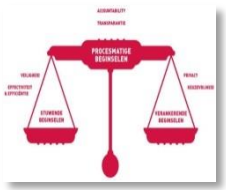
"How does the Commission define the term 'abnormal behaviour' used in the [INDECT research] programme?" – European Parliament, 2009

iOverheid (*iGovernment*) - http://www.ioverheid.nu/



Pro-active security = cheaper security

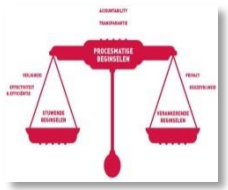
- Preparation
- Prevention
- Caught in the act
- Crisis response
- Investigation
- Acceptance



Pro-active security = cheaper security

- Preparation
- Prevention
- Caught in the act
- Crisis response
- Investigation
- Acceptance

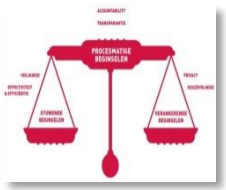
Later in the incident ➔ increasing costs



Criminal phases

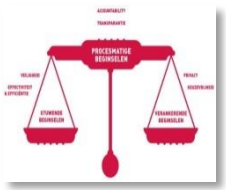
- Broad target selection
- Intelligence and surveillance
- Specific target selection
- Pre-attack surveillance & planning
- Attack rehearsal
- Execution: actions on objective
- Escape & exploitation

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



Criminal phases

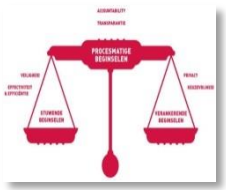
- Creating motivation
- Broad target selection
- Intelligence and surveillance
- Specific target selection
- Pre-attack surveillance & planning
- Attack rehearsal
- Execution: actions on objective
- Escape
- Exploitation
- Repent
- Rehabilitation



Criminal phases

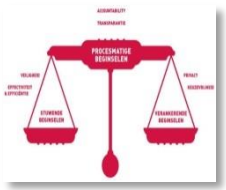
- **Creating motivation**
- **Broad target selection**
- **Intelligence and surveillance**
- **Specific target selection**
- **Pre-attack surveillance & planning**
- **Attack rehearsal**
- **Execution: actions on objective**
- Escape
- Exploitation
- Repent
- Rehabilitation

Proactive security



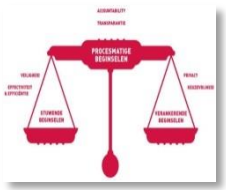
Effectiveness of security

Security processes / Criminal phases	Preparation	Prevention	Intelligence	Disturb	In the act	Investigate	Recover
Execution							



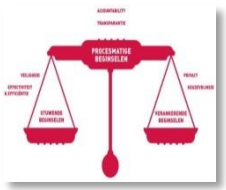
Effectiveness of security

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							



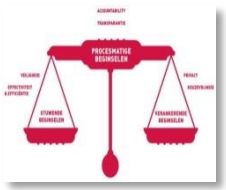
Effectiveness of proactive security

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							



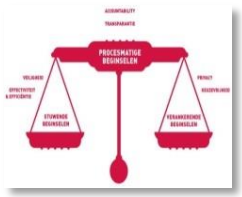
Example: effectiveness of CCTV

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



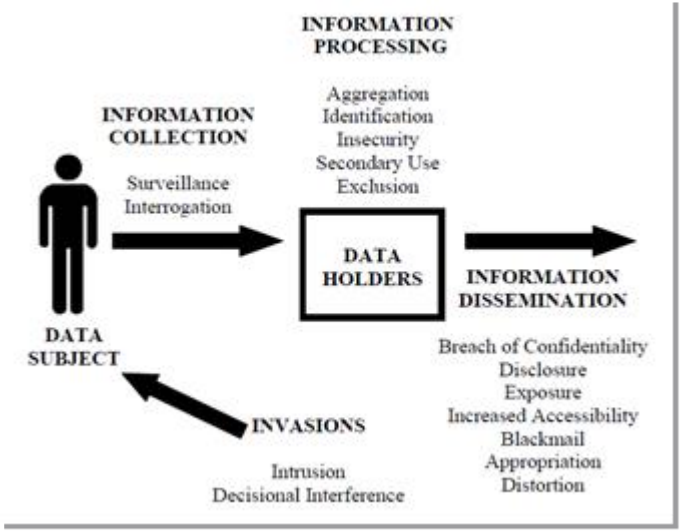
Effectiveness of proactive security

Security processes / Criminal phases	Preparation	Prevention	Intelligence	Disturb	In the act	Investigate	Recover
Create motivation							
Broad target selection	C	C	C				
Intelligence and surveillance	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

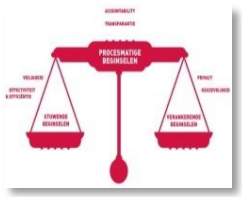


Invasiveness

- 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)

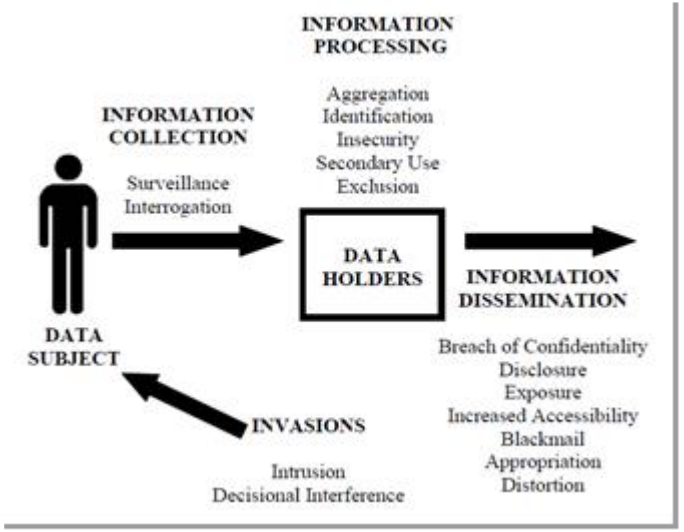


Solove, A taxonomy of privacy, 2006



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

TNO innovation for life

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

TNO innovation for life

Invasiveness				Description
A	None	0	None	There is no surveillance
B	Slight	1	Knowi	ee, 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 g device;
		4	Acting	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

Minimize invasiveness for normal (desired) behaviour.

Maximize the invasiveness for undesired behaviour.

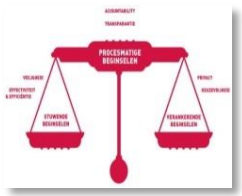
TNO innovation for life

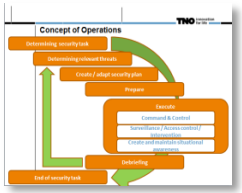
Invasiveness				Description
A	None	0	None	There is no surveillance
B	Slight	1	Knowi	ee, have to carry or do (e.g. you assume that a certain fraction of the subjects carries phones which you can monitor);
		2	Seeing	The subject sees the devices monitoring him around him, but he does not have to carry 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 g device;
		4	Acting	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

SECURITY-BASED SERVICE

Minimize inva (desired) behaviour.

Maximize the invasiveness for undesired behaviour.

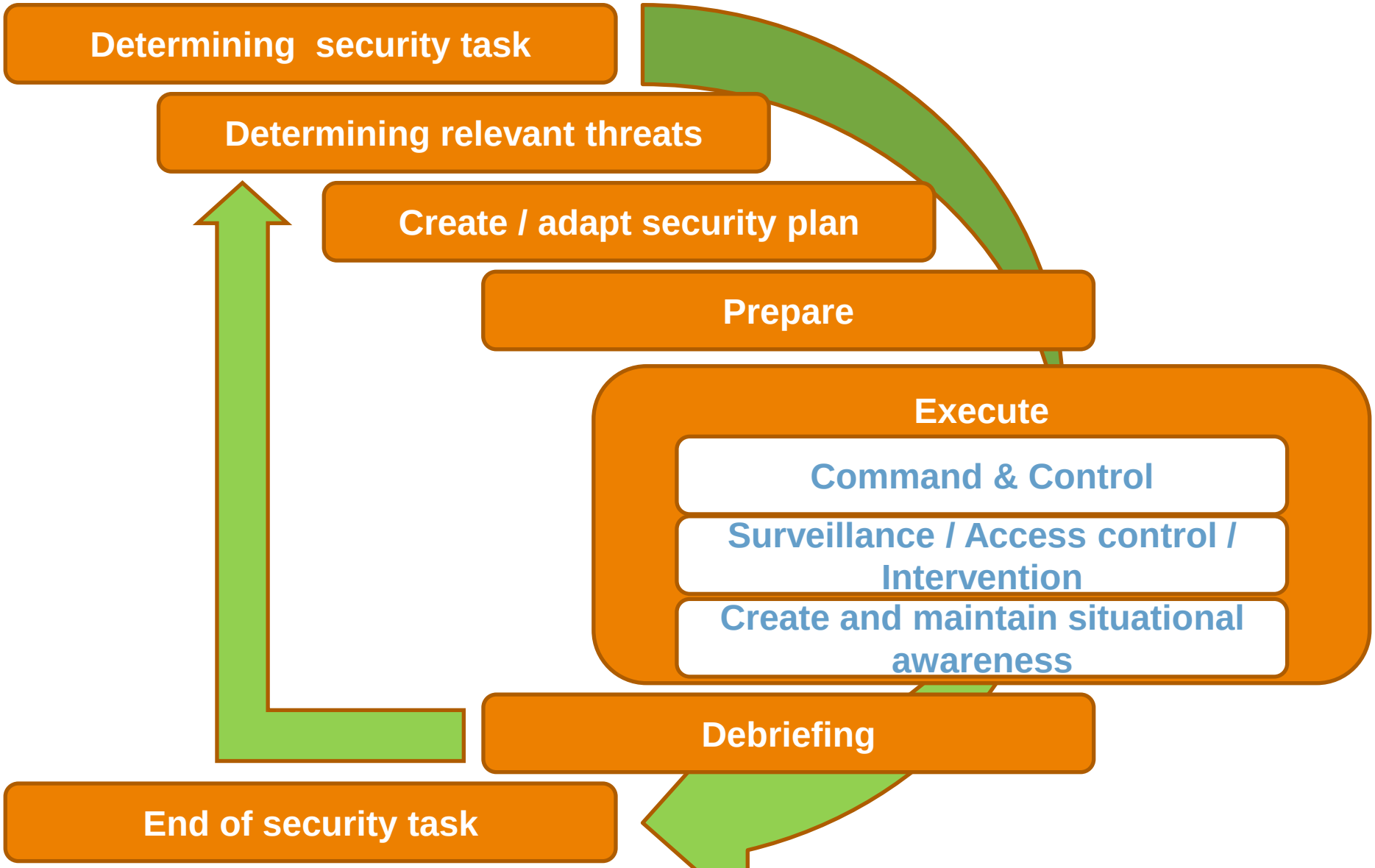




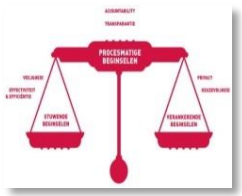
How to use deviant behaviour?

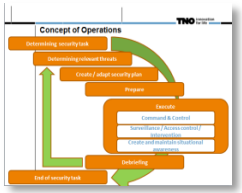
TNO innovation for life

Concept of Operations



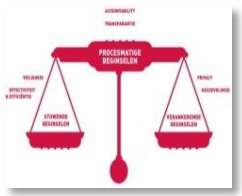
ConOps Step	Application of knowledge of deviant behaviour
Determining security task	Specify the object of security, its context and environment; Specify relevant normal behaviour, among them, but not limited to, the work processes of which the continuity must be protected; Specify levels of transparency, accountability, efficacy en efficiency;
Determining relevant threats	Specification of threats in specific modus operandi
Create or adapt security plan	Selection of definitions of deviant behaviour; Selection of methodology for specifying deviant behaviour (profiles); Specify deviant behaviour (e.g. with the help of local observation), including validation of this specification in the respective environment and contact; Creation of a security plan which can monitor, detect, recognize and identify these behaviours with satisfactory accuracy, in the desired phases of security (prevention, in-the-act, investigation).
Prepare(implementation of security plan, training)	Training of personnel in face to face behavioural profiling; Install security measures;
Execute	Secure the object of security on an operational level
Command & control	Introduce real life training simulations (“red teaming”, etc.); Periodic management reporting about efficacy, costs and impact on the liberty of the object of security;
Surveillance, Access control, intervention	Detection of normal and deviant behaviour; When intervening, take inaccuracy of surveillance into account with regard to the intentions of subjects;
Create and maintain situational awareness	Detection of relevant new normal and deviant behaviours; Determining that a certain threat is occurring;
Evaluation (debriefing)	Update knowledge of normal behaviour and processes, and of known modus operandi; Identify flaws in security plan;
End of security task	Transfer and store knowledge w.r.t. actual incidents and discovered modus operandi for next security task, i.e. facilitate learning;

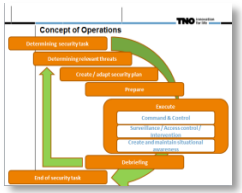




Nine definitions of deviant behaviour (1-4): threat based

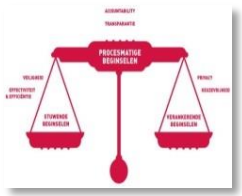
- Behaviour which may lead to dangerous and/ or undesired situations, i.e. which threaten the continuity of the processes at the location;
- Behaviour which correlates significantly with incidents;
- Behaviour which is part of the modus operandi of a criminal act;
- Behaviour which has as purpose to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

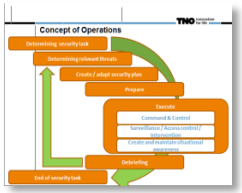




Nine definitions of deviant behaviour (5-9): continuity based

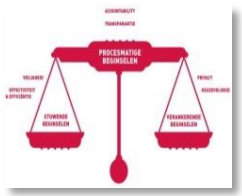
- Behaviour which is not part of any of the allowed (work-)processes which occur at the respective location or object;
- A reaction which does not fit to the stimulus if the intent of the subject were benign;
- Behaviour which falls outside the normal distribution of behaviour at the respective location;
- 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.

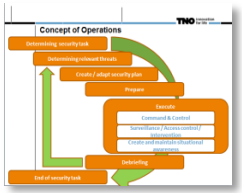




Indicative behaviour of pickpocketing

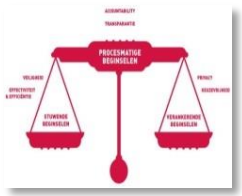
Aart Beukers – Eye-D Security Experts &
Dutch National Police

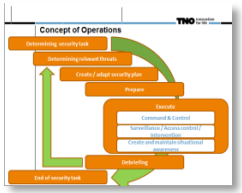




Modus Operandi map (MOmap)

MOMAP Pickpocket							
In the pickpocket scenario generally one or more (two is common) pickpockets work together. They are usually opportunistic criminals, selecting victims based on their vulnerability and likelihood for loot.							
Modus Operandi							
Time							
Persons en and objects							
Actions and events							
Possible interventions and stimuli							
Context							





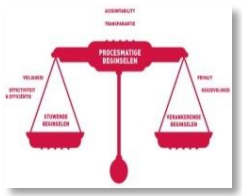
MOmap pickpocketing near tram

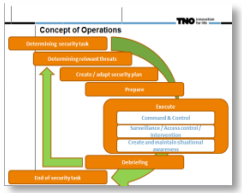
MOMAP Pickpocket							
In the pickpocket scenario generally one or more (two is common) pickpockets work together. They are usually opportunistic criminals, selecting victims based on their vulnerability and likelihood for loot.							
Modus Operandi	Looking for easy victim	Selecting victim	Position relative to victim	Distracting intended victim	Snatch valuable	Hide loot	Leave location
Time	10:05	10:30	10:31	10:31	10:31	10:31	10:32
Persons en and objects	P1, P2, P3	P1-P3, V3	P1, P2, V3	P1, V3	P1, V3	P1, P2	P1, P2, P3
Actions and events	Hanging around	Communication between P1, P2 and P3	Tram approaching	P1 is stalling the line	P1 snatches	P1 gives loot to P2	
Possible interventions and stimuli	Introduce fake victim	Approach victim to ask for route	Move in between P1 and V3	Distract P1 or P2	Caught in the act	Caught in the act	Caught in the act
Context	The location is Amsterdam. The scenario was put in scene by the Amsterdam police with actors.						

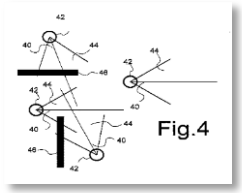
TNO innovation for life

Biases in surveillance

Bias name	Description
Funding bias	The tendency of scientists (and of police and intelligence officers?) to prevail the outcome of studies which support the interest of (financial) sponsors.
Law of the instrument	Too much trust in a specific tool or resource
Positive feedback	A self-influencing effect in a system.
Recall bias	The systematic error that people make when remembering events.
Reporting bias	The error that people make when reporting events.
Surveillance bias	The phenomenon where people pay more attention to a specific selection of people than to others.
Conformity bias	The tendency of people to let prevail information which confirms their believe (case building).
Exclusion bias	The systematic exclusion of certain (types of) subjects.



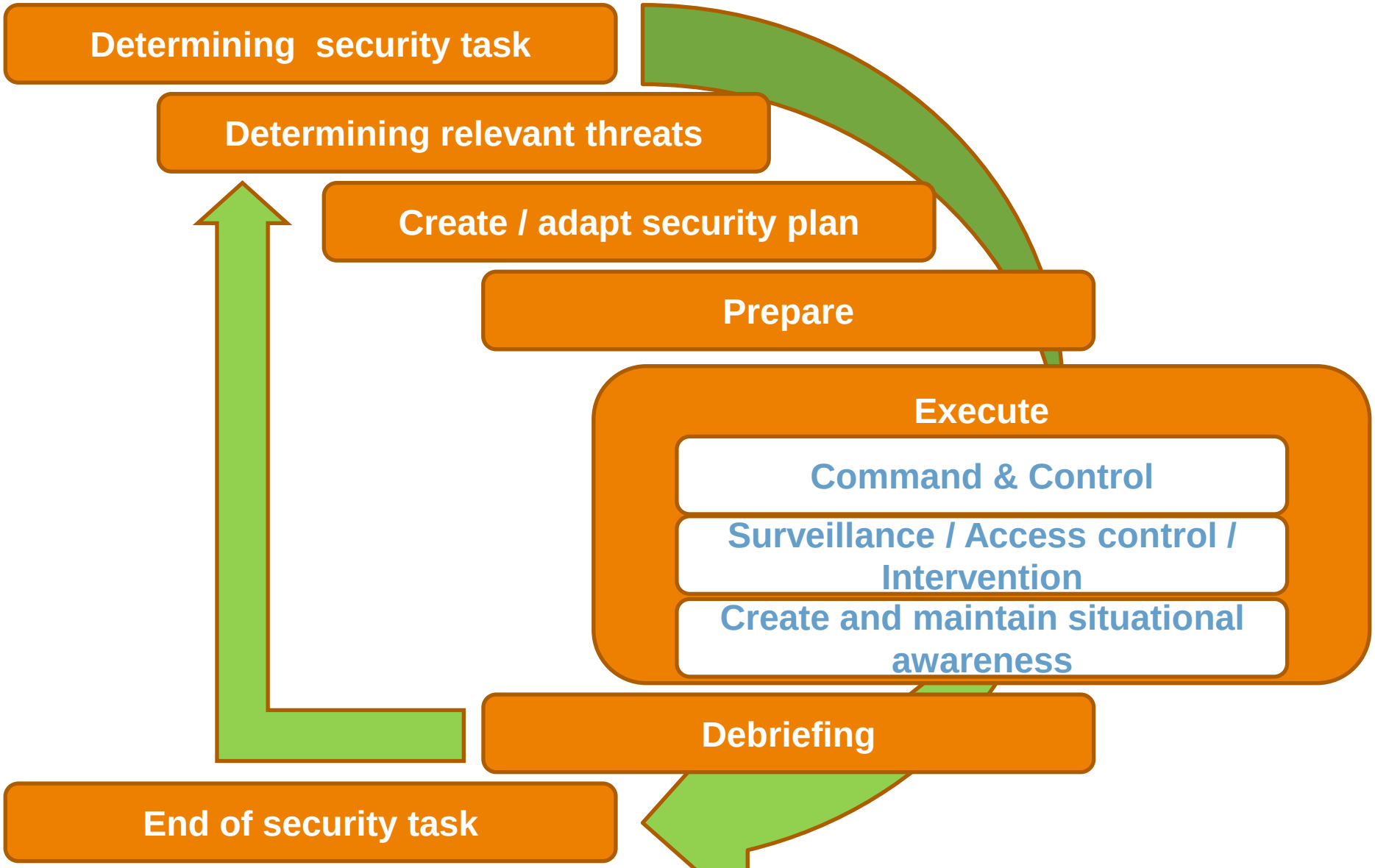


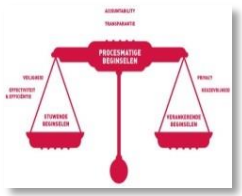


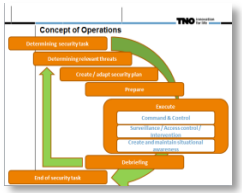
What to do to use deviant behaviour?

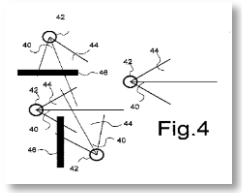
TNO innovation for life

Concept of Operations





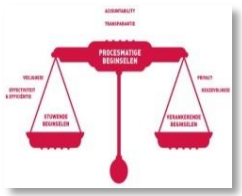


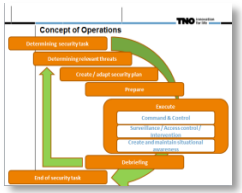


Predictive behaviour profiling

Rouse him, and learn the principle of his activity or inactivity.

– Sun Tzu ~500BC


PROCESMATIGE BEGINSELEN


Concept of Operations

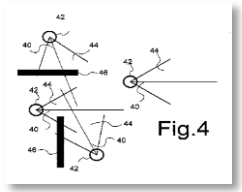
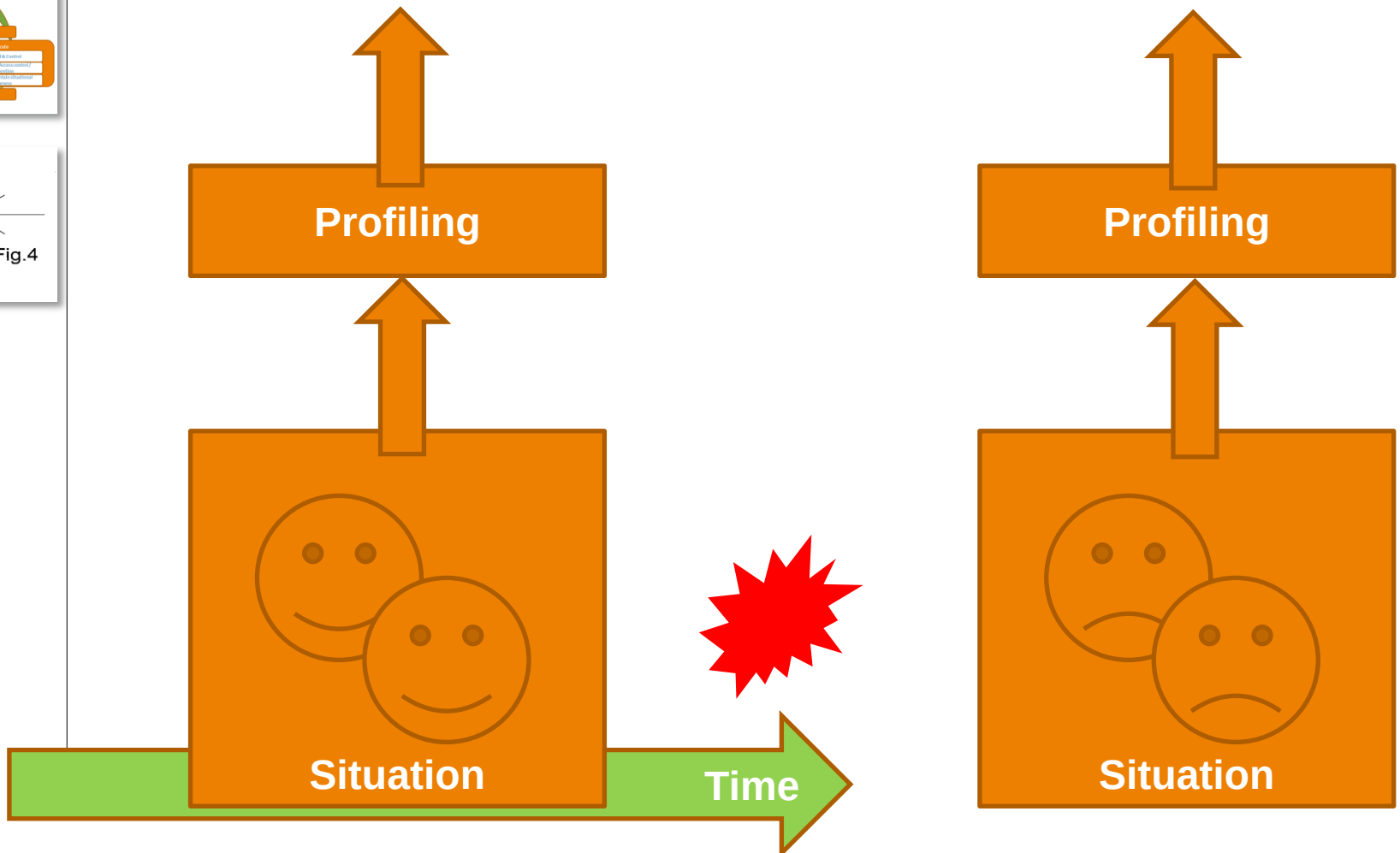
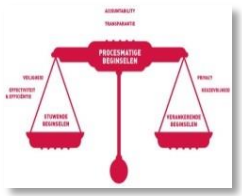
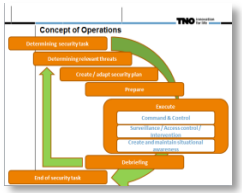


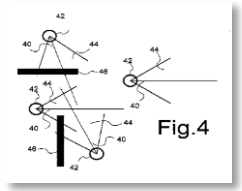
Fig.4

Profiling


Profiling
Profiling
Situation
Time
Situation

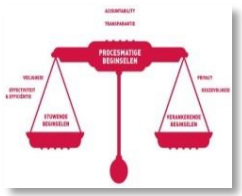


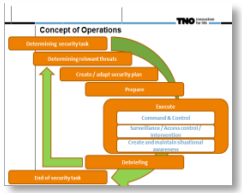


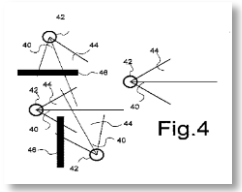


Types of profiling

Types of profiling	Examples	Description
Pre- or post incident	Predictive profiling	Determine the chance that an incident will happen. Optional: with the object of profiling as cause.
	Offender profiling; Criminal profiling	Determine the chance that the object of profiling was involved in a crime.
Input of profiling	Behavioural profiling	To use information about behaviour as input of profiling.
	Racial profiling	To use information about race as input of profiling.
Output of profiling	Geographic profiling	To determine the location of residence or work of a (potential) offender.
Domain	Cybercrime profiling	To use profiling to prevent or solve cybercrime.
Object of profiling	Person	Profiling persons, e.g. before boarding international flights.
	Group	Profiling groups of people, e.g. in crowd management.
	Situation	To determine whether a situation is suspicious without singling out one (group of) persons.

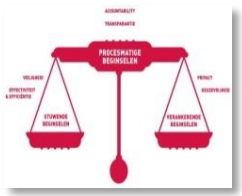


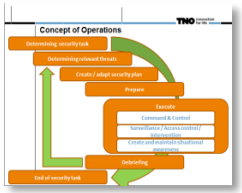


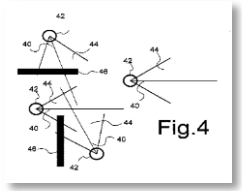


Predictive behaviour profiling

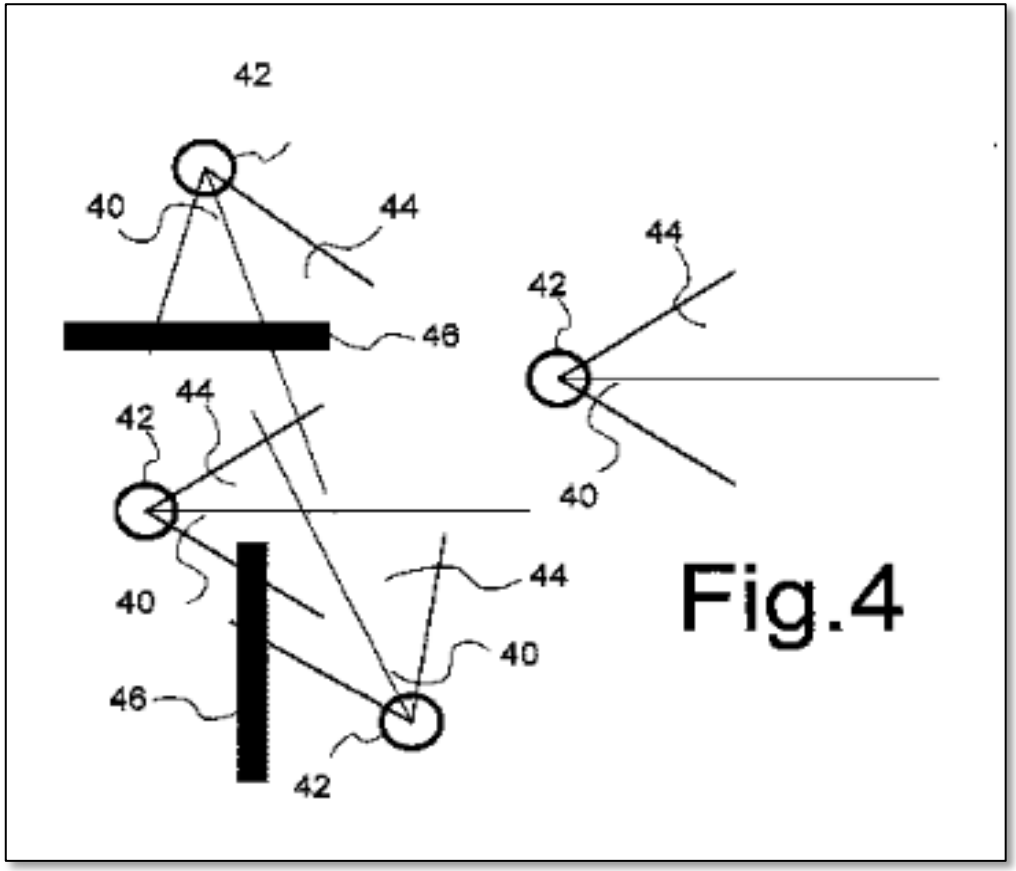
Types of profiling	Examples	Description
Pre- or post incident	**Predictive** profiling	Determine the chance that an incident will happen. Optional: with the object of profiling as cause.
	Offender profiling; Criminal profiling	Determine the chance that the object of profiling was involved in a crime.
Input of profiling	**Behavioural** profiling	To use information about behaviour as input of profiling.
	Racial profiling	To use information about race as input of profiling.
Output of profiling	Geographic profiling	To determine the location of residence or work of a (potential) offender.
Domain	Cybercrime profiling	To use profiling to prevent or solve cybercrime.
Object of profiling	**Person**	Profiling persons, e.g. before boarding international flights.
	Group	Profiling groups of people, e.g. in crowd management.
	Situation	To determine whether a situation is suspicious without singling out one (group of) persons.



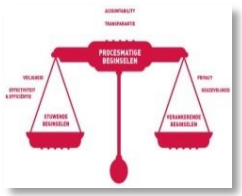


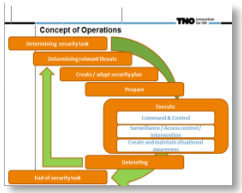


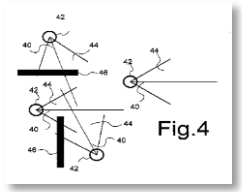
Proactive analytics



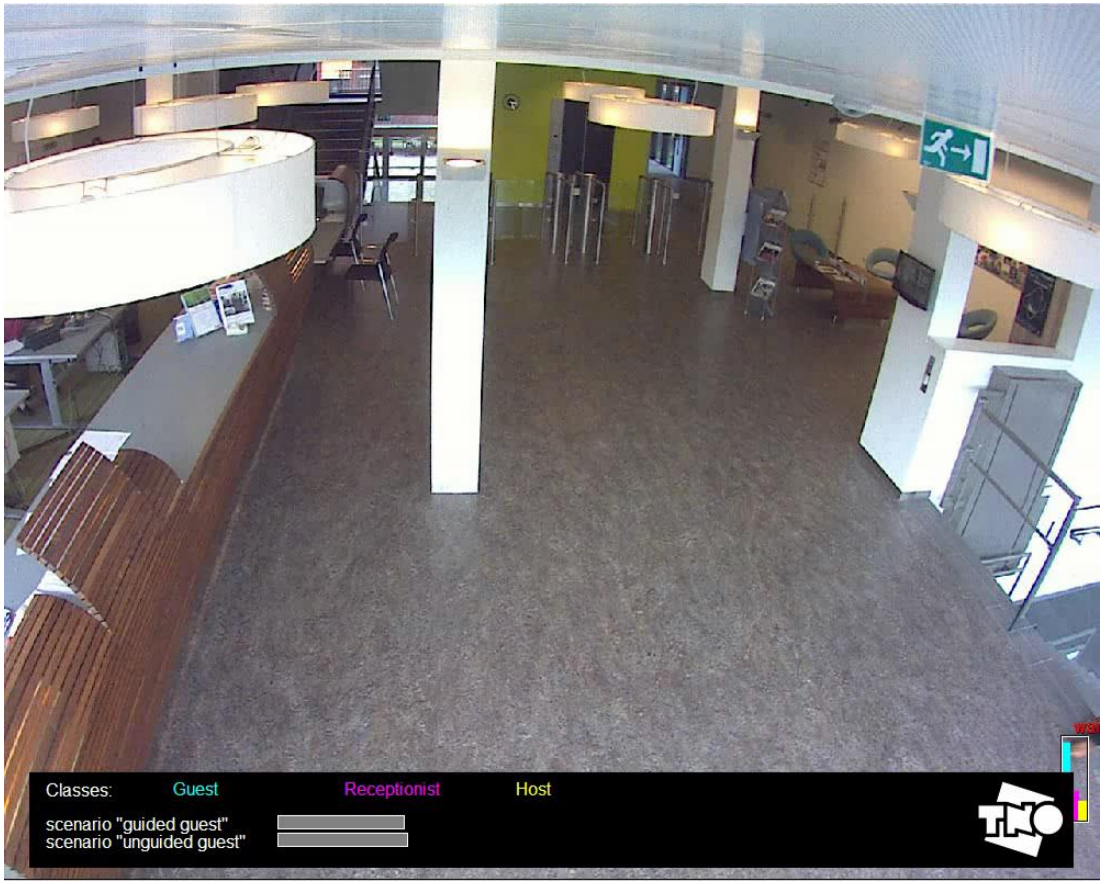
Patent WO2013036129 (A1)

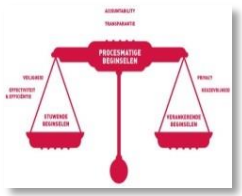


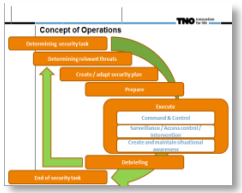


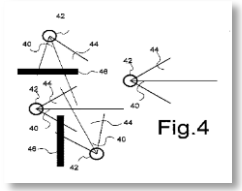


Proactive analytics



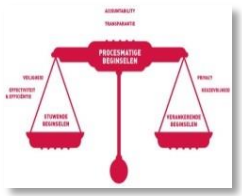


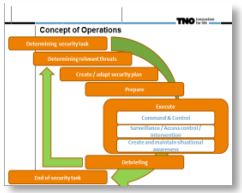


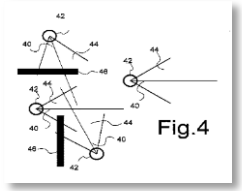


Automatic predictive analytics of pickpocketing

- Pickpockets switch between loitering and observing passers-by, and blending in with the moving crowd
- Collaborating pickpockets meet each other sometime with, and sometimes without acknowledging each other
- Pickpockets move into the personal space of others, without being acknowledged there
- Pickpockets take something out of someone else's bag or coat



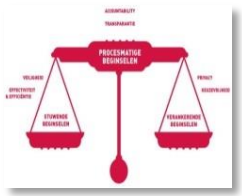


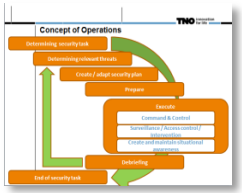


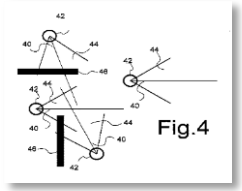
Automatic predictive analytics of pickpocketing

- Pickpockets switch between loitering and observing passers-by, and blending in with the moving crowd
- Collaborating pickpockets meet ea… …ometime with, and sometimes without ackn… …each other
- Pick… …ove into the personal space of others, without being ack…owledged there
- Pickpockets take something out of someone else's bag or coat

More specific = more difficult to observe (?)



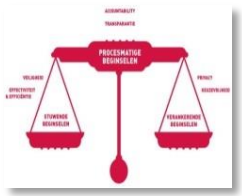


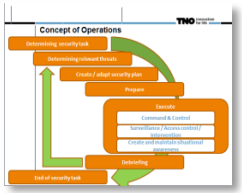


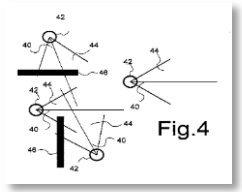
Dataset of 30 pickpocket incidents in shopping mall

- 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

ERNCIP
EUROPE 2020
European Reference Network for Critical Infrastructure Protection
the project





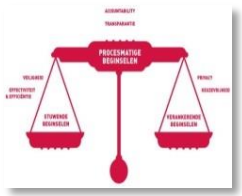


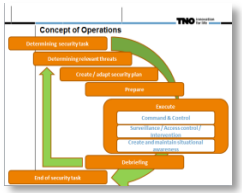
Predictive behaviour profiling training

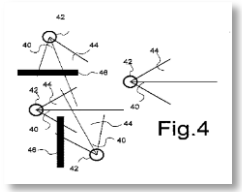
(Behaviour, Intentions) =

Context (Environment(Response (Cognitive agent (Intentions, Stimuli)))

- Behaviour and intention are two different things;
- A person has intentions;
- A person reacts to stimuli: current or past;
- This reaction can only be expressed in the environment of the person;
- This environment has a context;
- Intentions can be changed based on stimuli.





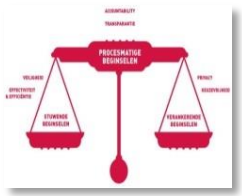


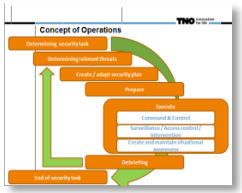
Predictive behaviour profiling training

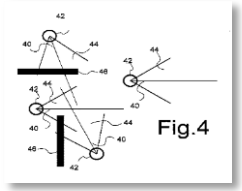
(Behaviour, Intentions) =

Context (Environment(**Response** (Cognitive agent (Intentions, Stimuli)))

- Behaviour and intention are two different things;
- A person has intentions;
- A person **reacts** to stimuli: current or past
- This reaction can only be expressed in the environment of the person;
- This environment has a context;
- Intentions can be changed based on stimuli.

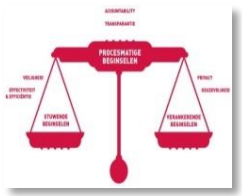


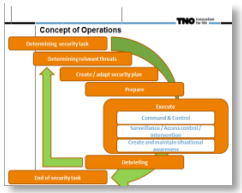


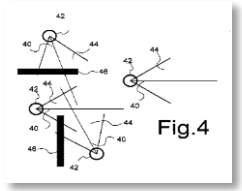


Harmonisation in training programs

- Terms and definitions
- Working principles (validation of efficacy)
- Customization to local context and environment
- Interoperability, with
  - other training bureaus;
  - other security organisations;
  - with technology.
- Integration in concept of operations (validation of effectiveness)

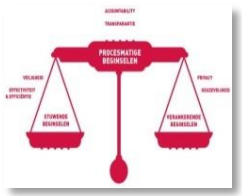


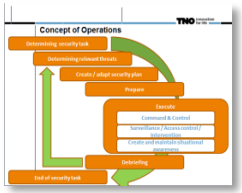


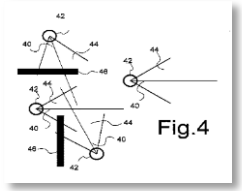


Recap

- Why?
  - Proactive = cheaper
  - Effectiveness
  - Invasiveness
- How?
  - Concept of operations
  - Definitions of deviant behaviour (both generic and specific)
  - Awareness of biases
- What?
  - Predictive behaviour profiling
  - Behaviour analytics
  - Proactive security training programs

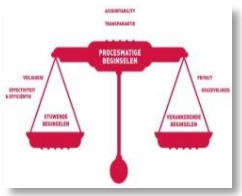


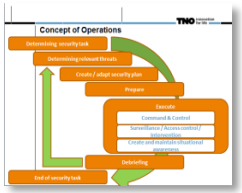


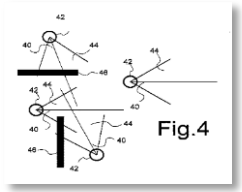


Take-home message

- Integrate vertically on all governance levels
  ➔ with your clients!
- Integrate in concept of operations in all steps
  ➔ with all relevant participating organisations for your assets!
- Harmonize your market in order to mature and grow
  ➔ with your peers!







Sources

- Dutch National Programme on High risk object security
- EU FP7 Tactical Approach to Counter Terrorists in Cities (TACTICS: fp7-tactics.eu)
- Dutch National Top-sector High-tech Systems & Materials “Passive Sensors”
- TNO Research programme on Deviant Behaviour

TNO innovation for life

ONGERUBRICEERD

Behavioural and Societal Sciences
Oude Waalsdorperweg 63
2597 AK Den Haag
Postbus 96864
2509 JG Den Haag

www.tno.nl

T +31 88 866 10 00
F +31 70 328 09 61

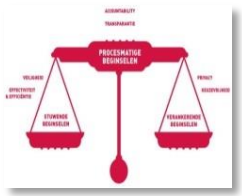
TNO-rapport

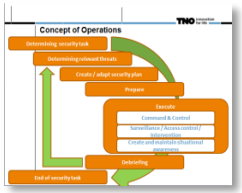
Afwijkend Gedrag
Maatschappelijk verantwoord waarnemen van gedrag in de context van veiligheid

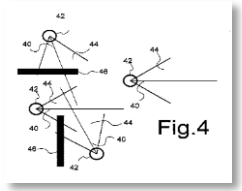
Datum 15 februari 2014
Auteur(s) Jeroen van Rest, Maaike Roelofs, Anna van Nunen
Exemplaarnummer
Oplage
Aantal pagina's 158 (incl. bijlagen)
Aantal bijlagen
Opdrachtgever Bert Don
Projectnaam VP Veilige Maatschappij 2011-2014
Projectnummer 060.07961

ONGERUBRICEERD

Koninklijke Marechaussee · POLITIE · TACTICS · Holland Pioneers in international business · ERNCIP European Reference Network for Critical Infrastructure Protection the project







Recommendations

- **Security-based service**: create a hinder-index for your security measures based (in part) on invasiveness in order to better understand (a lack of) support of your end users.

- **Share modi operandi with your peers** in a systematic and secure manner in order to practice pro-active security, to be able to describe effectiveness of (pro-active) security measures.

- **Use specific measures of effectiveness** which distinguish between effectiveness *before the crime* and effectiveness *during the crime.*