Earth, life and social sciences
Oude Waalsdorperweg 63
2597 AK Den Haag
P.O. Box 96864
2509 JG The Hague
The Netherlands

www.tno.nl

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

Extended Summary

| Final report

Deviant behaviour - Socially accepted observation of deviant behaviour for security - extended summary

Date	12 September 2014
Author(s)	Jeroen van Rest, Maaike Roelofs, Anna van Nunen
Copy no	
No. of copies	
Number of pages	27 (incl. appendices)
Number of appendices	
Sponsor	Bert Don
Project name	Deviant Behaviour
Project number	060.07981

Contents

1 Introduction

This extended summary summarises the results of a work package in the project “Recognising Deviant Behaviour” in the demand-driven Secure Society programme.

The question being studied is “what factors influence the support for proactive surveillance and how can this support be improved?” The methodology comprised a combination of literature review, interview, questionnaire and validation by scientific peer review of defined components.

This summary is intended to be used as a reference in further communication about the results and recommendations of the work package. The complete results are reported in Dutch [22]*. Additional English references were added to this summary. The results were also presented at the 2014 ASIS Europe conference [25].*

This work is based on the premise that a better understanding of deviant behaviour enables better choices to be made in safeguarding and organising security (and thus freedom) whereby public support for proactive surveillance is maintained and/or boosted.

The recognition of deviant behaviour offers the possibility to see security incidents approaching and to intervene in time. This is only socially acceptable if done ethically and does not, for example, result in ethnic profiling and other forms of discrimination by (external) features that are unconnected with a criminal act or incident. To this end a methodical approach is needed, including the establishment of clear terminology and work processes along with scientific validation in the field. This summary describes this methodical approach as established by TNO in the project “Recognising Deviant Behaviour”. The results are directly relevant to security in both the physical and digital space.

The application of knowledge about deviant behaviour concerns various stakeholders: citizens, administrators, politicians, supervisors, emergency services (public and private) including the police and Royal Military Police, and all kinds of companies. Knowledge about deviant behaviour can help stakeholders on roughly three levels:

- strategic (why / direction),
- tactical (what / content) and
- operational (how / execution).

This summary describes a range of recommendations at each of these levels aimed at maintaining and boosting support for proactive surveillance. The key recommendation is the development of specific, empirically based effectiveness measures for use with proactive methods of surveillance. A methodical approach is needed for effective validation.

A clear set of terms and definitions is essential to enable reasoning about (deviant) behaviour and thereby enhance the political and social debate, the design and structure of surveillance systems and operational cooperation as well as communication with suppliers of training, tools and systems. Definitions of terms like (deviant) behaviour, profiling and invasiveness are considered at length in this report.

1.1 Security versus privacy?

A civilised society chooses to protect freedom. The juxtaposition that exists between security and privacy (a form of freedom) is due to the need for surveillance in order to prevent citizens becoming a danger to themselves or others, either on purpose or by accident, thereby limiting their freedom. When such a risk exceeds the *accepted risk*, society demands that government protects citizens from each other or from external threats. And so everyone gives up a bit of individual freedom to maintain collective freedom. The flip side, of course, sees the freedom of the individual vying with the freedom of the collective. A society with 100% privacy would thus be a very insecure society. The development of knowledge about deviant behaviour is based on the premise that this will enable society to remain safe and secure and, therefore, free, provided that the use of this knowledge takes adequate account of the ethical issues.

1.2 Necessity of observing deviant behaviour

Surveillance is used as a means to tackle a wide spectrum of security problems, such as human trafficking, drugs smuggling and drugs trade, theft, raids, high-risk object security and events security.

With the current societal emphasis on preventing incidents, pressure is growing to predict incidents correctly and early. The recognition of deviant behaviour of people at an early stage provides the possibility to catch people in the act or even to interrupt or prevent incidents, or at least reduce their effects. This feeds the need to better understand what deviant behaviour is and how it can be recognised.

Familiar indicators of involvement in criminal activity like age, gender, ethnic origin and level of education are neither precise not complete. In addition, they say nothing about when the crime might happen. So there is an opportunity here to gain greater insight. After all, there are all kinds of factors that can be the basis for suspecting a person or situation. It can be argued that information about behaviour is the best kind of predictive information because there is no crime without behaviour. The behaviour is also important because it:

1. is conditional for the actual occurrence of the incident;
2. makes the difference between thinking about a crime on the one hand and preparing and committing the crime on the other, with all its legal consequences;
3. gives a practical handle in time, place and individual(s) for a reaction aimed at prevention, detection, interruption, enforcement or emergency assistance;
4. has an explicit place in the field of criminality: *modus operandi* means *way of operating.*

1.3 Terminology

Shared understanding of relevant terminology is a precondition to fruitful discussion, research and design. In the domains of police, surveillance, behaviour psychology and system engineering there are several concepts which are notoriously poor understood. The aim of this section is to provide the definitions which are used in the remainder of this extended summary.

Term	Definition
Agent	An agent is an autonomous entity such as a human, an animal and an automated self-controlled system (a robot). In this report it means a person in the role of victim, witness, perpetrator or supervisor.
Asset (to be protected)	The object, person, situation or the process of which the continuity must be protected. This can be e.g. the life and wellbeing of a VIP, the democratic order or public order in general.
Behaviour	The reaction of a cognitive agent to a stimulus, expressed in elements of his environment.
Behaviour profiling	The extrapolation of information about a cognitive agent, based on its behaviour.
Bias	Bias is a systematic flaw in judgment, caused by a distorted image of reality. Biases are common to all humans and can pertain to attention, information processing, attribution, categorization of groups, patterns, and contextual factors such as fatigue and noise. Prevalent examples of cognitive biases are the confirmation bias, which is the tendency to seek information that corresponds with pre-existing ideas or to interpret information in such a way that it verifies pre-existing ideas [18], and stereotyping, which involves describing a person in terms of (often negative) characteristics of the group this person belongs to [6]. For an overview of cognitive biases see Baron [1]. The Dutch report contains a separate overview of relevant biases in appendix H [22].
Cognition	The ability to solve problems.
Context	The context of a surveillance system consists of the factors that influence the system and necessarily includes the environment, including people in the environment. Typical examples of surveillance context are the local culture, the level of threat, and the weather conditions. Additionally, world knowledge as prior probability, and known correlations between events and actions, are also a part of a surveillance system’s context.
Deviant behaviour	There are many kinds of deviant behaviour. See Chapter 5 for nine different perspectives on deviant behaviour, and for a collection of methods to specify deviant behaviour.
Effectiveness	The degree to which a desired effect is obtained. See also *efficacy*.
Efficacy	The degree to which a desired effect is obtained in controlled circumstances, like in an experiment. See also *effectiveness*.

Environment	(1) The environment of a system is the system’s surrounding that could interact with the system. The typical environment for a surveillance system is the area under surveillance including the people under surveillance and the location(s) of the system components (including storage, data transport, monitoring room etc.). (2) The environment of a subject is those factors that have direct interaction with it.
Intent	The state of mind of a cognitive agent (a person) which is directed towards an object or situation in his environment.
Invasiveness, intrusiveness	The degree to which the integrity of a person is breached. This has both an objective and a subjective component. Invasiveness of surveillance measures can be related to five different aspects: • the extent to which the individual loses autonomy; • the degree of detail of the data that is recorded; • the by-catch of other subjects unrelated to the threat or the asset to be protected; • the legality (e.g. surveillance for the purpose of espionage); • the transparency; See Chapter 3 for more information.
Privacy	Privacy is the ability to control and limit physical, social, psychological and informational access to the self or one’s group [4]. Gutwirth writes that privacy is the safeguard of personal freedom--the safeguard of the individual's freedom to decide who she or he is, what she or he does, and who knows about it [10]. Langheinrich gives a short history of the concept of privacy by design [12], and illustrates as part of that history the origination of five specific categories of privacy that together appear to encapsulate all previous definitions: • Privacy of personal behaviour (media privacy); • Privacy of territory (territorial privacy); • Privacy of the person (bodily privacy); • Privacy of personal communications (interception privacy), and • Privacy of personal data (data or information privacy). The definition of privacy –in relation to data protection- is not settled.
Privacy by Design (Data protection by design)	The principle of ‘Privacy by Design’ means that privacy and data protection are embedded throughout the entire life cycle of technologies, from the early design stage to their deployment, use and ultimate disposal [24].
Prodding actions	(Dutch: prikkelen) Prodding is a kind of behavioural profiling which consists of the active variation of stimuli on one or more persons. It is typically used to assess the intent of the subject.

Profiling	The extrapolation of information about something, based on known qualities. It leads to the identification of patterns in data of the past which can develop into probabilistic knowledge about individuals, groups and situations in the present and in the future [11]. See section 6.2. Profiling can be categorised in different manners. This report elaborates on predictive behavioural profiling.
Risk	A risk is the combination of the chance on, and the impact of an undesirable situation. A risk is caused by the combination of an asset, a threat and a vulnerability. Accepted risk is risk that is accepted in a given context based on the current values of society or in the organisation.
Safety and security	Safety is the absence of risk. Security is the absence of risk caused by others.
Scenario	A scenario is a synoptical collage consisting of a meaningful series of actions and events.
Sensor	A device which converts one energy to another, usually an electric signal, e.g. microphone, CCTV camera, pressure sensor and also the human eye. There are several closely related concepts: An active sensor sends a signal which is reflected by the subject, and/or which triggers a response from the subject, e.g. radar, sonar and lidar. An intelligent sensor applies some form of knowledge to either improve the output signal or to interpret the signal to a higher level of abstraction, e.g. a face recognition system, video content analysis and also a human. A probing sensor is a sensor with a probing mechanism with the function of bringing a stimulus to the observed subject. The response to the stimulus is measured by the sensor. Human surveillance professionals do this e.g. in security questioning.
Stimulus	A stimulus is a detectable change (as perceived by the subject) in the environment (including the subjects own body). A stimulus can already be present in the environment (with the subject passing by), or it can be introduced directly or indirectly by the supervisor. Varying stimuli are used in security questioning and predictive behaviour profiling to trigger a tell-tale reaction.
Subject	(In this report) The person under surveillance.
Supervisor	The person that is tasked with surveillance. This is typically an educated professional in service of a security organisation or department.
Surveillance	The focused, systematic and routine attention to personal details for purpose of influence, management, protection or direction [16].
Suspicion	The feeling that a situation or a person is involved in a (specific) crime.
Threat	(That which leads to) the potentially occurrence of an undesirable situation. Security measures protect against threats.
Vulnerability	A weakness or hole in the security.

2 Effectiveness of security measures

Various surveillance methods exist to provide early warning of deviant behaviour. In order to describe their usefulness, a clear definition of the effectiveness of (proactive) security measures is necessary. However, this is complicated due to the following six factors.

First of all, it is often impossible to attribute the absence of a threat occurring to a specific security method. This is a fundamental problem of many effectiveness studies in criminology and is typically recognised by the use of a pre- and post-measurement, a measurement after a period of time (whether the effect persists) and a comparison with a similar alternative location (as described, for example, in the *Maryland Methods Scale*, level 3 [7]).

Secondly, and specifically for surveillance measures, the fact is often missed that it is only the information position that is improved in a narrow sense and incidents are not prevented or criminal investigations solved in themselves. The effectiveness of surveillance measures must, therefore, initially be described in terms of creating a correct and up-to-date overview. If the effects “on the street” also really have to be considered, then the effectiveness of the processes that make use of the overview gained must also be reviewed: the decision-making and intervention processes.

Thirdly, many kinds of threat occur so sporadically that no statistically significant conclusions can be drawn from the data. This, then, questions whether additional security measures are required for these threats. Sometimes, however, the impact is so high that this is indeed the case (for example, terrorism [19]).

Fourthly, specifically for *proactive* security measures, it is impossible to proof the prevention of a specific future incident. If there is an actual threat, intervention is the ethical thing to do, because it is then unethical to refrain from intervening just to find out whether a crime will be committed.

The fifth factor concerns the fact that the gradual development of incidents is often ignored in ascertaining the effectiveness of security measures. For instance, the transposition of crime is sometimes regarded as something negative [8] while this is actually a sign of an (desirable) effect on one of the earliest phases of crime: general target selection.

Finally, the effectiveness of a measure is not the same for different security tasks. For example, the effectiveness for the purpose of detection is quite different from the effectiveness for the purpose of crime prevention, something that has been recognised to some extent by Lum in the “*evidence based policing matrix*” [15].

If one or more of these six factors are misjudged, that could negatively impact the support for security measures, and specifically for proactive surveillance. After all, why employ them if their effectiveness cannot be ascertained? So, a more specific definition of the effectiveness of security measures is needed.

To this end we propose using an *effectiveness matrix*. One axis contains the processes needed to ensure security before, during and after an incident. The other axis contains the phases a criminal goes through to commit an incident.

The effectiveness of security measures is the extent to which:
1 the intelligence, enforcement (including prevention, interruption and being caught in the act) and incident detection are achieved.
2 potential criminals are inhibited or even stopped at a certain criminal stage.

For surveillance measures there is a third element, being the extent to which:
3 the measure contributes to a function of the process, such as obtaining an actual situational awareness.

The first two levels of effectiveness (1 and 2) together cover a matrix, see Chart 1.

Chart 1 Effectiveness matrix of security measures: green cells are aspects of effectiveness. Other cells are logically excluded. Today's effectiveness studies emphasise the execution phase and the aspects interruption, caught in the act and detection (the framed part). However, the cells 'C' are those in which, for example, camera surveillance may be effective and is sometimes demonstrated as such.

Security processes Criminal phases	Preparation	Prevention	Intelligence	Interruption	Caught in the act	Detection	Recovery
Developing motivation	🟩	🟩	🟩	☒	☒	☒	☒
General target selection	C	C	C	C	☒	☒	☒
Intelligence and surveillance	C	C	C	C	☒	☒	☒
Specific target selection	C	C	C	C	☒	🟩	☒
Planning and target surveillance	C	C	C	C	☒	🟩	☒
Dry run	C	C	C	C	☒	🟩	☒
Execution	C	☒	☒	C	C	C	☒
Fleeing	C	☒	☒	☒	C	C	☒
Enjoying the fruits of the crime	🟩	☒	☒	☒	☒	🟩	☒
Repentance	🟩	☒	☒	☒	☒	☒	🟩
Rehabilitation	C	☒	☒	☒	☒	☒	C

The hypothesis for using the knowledge of deviant behaviour in security is that:
1 all security procedures can benefit, and
2 criminality can be stopped, or at least inhibited, early in its development.
Using knowledge of deviant behaviour in proactive surveillance is therefore mainly found in the upper left of this effectiveness matrix, i.e. up to execution / being caught in the act.

Of course, people may repent by themselves, so we must be aware that not all the effects are caused by the security measures themselves. But a meta-effectiveness study of security measures in general based on this new definition, and preferably in an international context, may boost support for security measures and help direct the research and development of new surveillance concepts.

2.1 Effectiveness versus efficacy

It is important here to make a distinction between *efficacy* and *effectiveness*. A security measure tried in a pilot project may well lead to the required effects (efficacy) but is unlikely to be effective in practice (no effectiveness) if not well integrated in all the relevant work processes (e.g. a lack of training) or where ICT support is not properly aligned to information flows. Since behaviour depends on many local and contextual factors, it is recommended to always validate the behaviour indicators in the respective environment and context, and to be cautious about taking over the results gained in a different environment and context.

3 Invasiveness

There is a lack of a common understanding of the concept of invasiveness. Invasiveness of surveillance measures can be related to five different aspects:

- the extent to which the individual loses autonomy, i.e. he has to cooperate with the surveillance;
- the level of detail of the data that is recorded;
- the by-catch of other subjects, or other locations, or other moments unrelated to the threat or the asset to be protected;
- the legal basis, e.g. surveillance for the purpose of espionage is more invasive;
- the transparency, e.g. surveillance without notification is more invasive.

Using this more specific definition, the invasiveness of a specific (surveillance) system can be described more specifically than is now typically the case, and thereby at least a qualitative comparison can be made between two alternative surveillance systems, or between an older and newer system. Citizens, politicians, surveillance staff and those placed under surveillance can also debate more specifically the required or experienced degree of invasiveness. The next section goes into even more detail, and provides *scales of invasiveness*.

3.1 Scales of invasiveness

This report provides a scale that comprises the first two aspects in Chart 2. The full report give more detail about the meaning of the levels.

Chart 2 Four- and nine-point scales of invasiveness.

Invasiveness (4 point)		Invasiveness (9 point)		Definition
A	None	0	None	No surveillance
B	Light	1	Know, not seen	The subject knows he is being observed but does not see it nor does he have to wear or do anything for this (for instance, normal camera surveillance is built into the environment)
		2	Seen	The subject sees the sensors that observe him, but he does not have to wear or do anything
C	Medium	3	Worn	The subject wears a device that is monitored, and so must cooperate. The device requires no further action. E.g. a GPS tracking device or mobile phone
		4	Do	The subject has to regularly do something to be monitored, such as provide biometrics in a controlled environment or present an RFID card to a reader
		5	Possibly interrupt	The supervisors have the option to interrupt what the subject is doing although this is not certain. For instance, a police officer adjacent to a flow of people or an access gate that is open but can close for particular subjects
D	Strong	6	Interrupt	The subject knows that what he is doing will actually be interrupted, for example, a reception desk with a waiting area at a secured building that he wants to visit.
		7	Available	The subject must allow physical access to (part of) his body, as in the case of a frisk
		8	Full transparency and cooperation	The subject allows full access to his body as well as measuring internal physiological parameters

These scales of invasiveness have not yet been coupled to a scale of “agreeability” or, otherwise, “nuisance”. For example, there may well be significant distance between two successive steps in terms of how agreeable one feels. Further research into this is recommended to be able to make better reasoned choices and thereby gain more support from society for use of surveillance resources. By more consciously taking account of the degree of invasiveness of surveillance measures security staff may be prompted to think of ways of making the surveillance less invasive.

3.2 Invasiveness of observing deviant behaviour

Given that the quality of observation depends on many factors, it is impossible to draw any general conclusion about “the degree of invasiveness needed to observe deviant behaviour”. If deviant behaviour is observed using probing actions (see section 6.2.2) then the invasiveness is typically level 5 or 6, but it can be much lower with other forms of deviant behaviour observation.

4 Deviant behaviour in work processes

Knowledge about deviant behaviour must be embedded in the work processes (Concept of Operations or ConOps) to be able to be applied. While a ConOps tends to be tailor-made, a generic version can be made for surveillance. Chapter 4 of the original report [22] indicates where and how in a ConOps knowledge about deviant behaviour can be applied for this purpose. An essential step of the ConOps is to validate the applied knowledge of deviant behaviour in terms of effectiveness: does it actually generate the required information? In any case, it makes sense to regularly check the effectiveness of the ConOps, given that people can adjust to the surveillance (both benevolently and maliciously), and certainly if there is a high turnover of surveillance staff because this means that experience is leaving the organisation quickly.

Once there is a concrete threat at a vulnerable or high-risk location, it is already too late to build up an objective picture of what is normal there. Communicating about the threat may cause the public, the surveillance staff and processes to behave differently. To prevent this, a pre-emptive picture of what is normal for such locations and locations can be drawn. Various methods in this report can be used to both draw a picture of deviant behaviour and generate a picture of what is normal.

If it is known exactly what behaviours are relevant or not, the performance of surveillance resources (personnel, technology) can be monitored and thus managed in a SMART way. In such a scenario, knowledge about deviant behaviour helps to improve surveillance concepts, including the reasoning and validation of design choices and investment decisions.

5 What is deviant behaviour?

There is no single definition of deviant behaviour. Different definitions are being used in the security domain alone. In order to understand the differences, a comprehensive description of behaviour is required. A "formula" that to some extent illustrates the complexity of behaviour is the following:

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

This formula prompts the user to:

1 see behaviour and intentions as two separate things;
2 always regard a cognitive agent (person) with one or more intentions (e.g. "I want to pickpocket someone");
3 always attribute an action or reaction (response) to a cognitive agent;
4 always regard this reaction as a consequence of one or more stimuli: also if at that moment it is not (yet) known which stimuli this concerns;
5 always express these stimuli, agent and response in terms of elements in the environment;
6 always give further context to this environment;
7 realise that intentions themselves can also be modified on the basis of new experiences (stimuli).

5.1 Perspectives of deviant behaviour

This report describes deviant behaviour according to the following contexts: security, ethics, the legal system, psychology, statistics and information theory. This ultimately produces nine different perspectives of deviant behaviour, which may be useful in different situations. Chart 3 shows these nine perspectives directly related to a pickpocketing example. The first four perspectives are reasoned on the basis of the notion that security relates to countering a specific threat. The other five are reasoned on the basis of the notion that security may mean the absence of threat. The full Dutch report contains four examples for which the relevance of these perspectives are elaborated.

Chart 3 Perspectives of deviant behaviour, with pickpocketing examples.

Deviant behaviour is the way a crime is committed, i.e. the modus operandi.	More modus operandi are known whereby pickpockets are adept.
Deviant behaviour is behaviour that has a high degree of correlation with incidents.	Certain (combinations of) action are suspected to be highly correlated with pickpocketing. Appendix I details this.
Deviant behaviour is behaviour that arises from mental strain.	During the pickpocketing incident it is essential to mimic normal behaviour and thus not be noticed. This may lead to high mental strain that may affect reflexes.
Deviant behaviour is the reaction to a stimulus whereby it is uncharacteristic of someone who has no malevolent intentions.	If someone unwittingly passes by and has the appearance of a person with valuables on him, this may been the stimulus to which a pickpocket reacts.
Deviant behaviour is behaviour whose purpose is to benefit at the expense of another: unethical behaviour.	Pickpocketing is not ethical since you gain at the expense of another.
Deviant behaviour is behaviour that may lead to dangerous or in any case undesirable situations (since it threatens the continuity of the primary processes).	The loss of valuables is already undesirable in itself but if the perpetrator is caught in the act, the situation may escalate and become dangerous. In general, people will feel less secure in locations where pickpocketing is prevalent, and may even avoid such locations (like railway stations, shopping malls or high streets) if they can.
Deviant behaviour is behaviour that deviates from normal social standards.	Stealing from someone is socially unacceptable. Certain aspects of some modus operandi even demand more subtle socially deviant behaviour, such as standing close together.
Deviant behaviour is behaviour that deviates statistically from normal behaviour.	The number of pickpocketing incidents is very low in relation to the number of times people shop.
Deviant behaviour is behaviour that does not come within the normal (operating) processes of the location or object.	No location or object exists of which the purpose is to facilitate pickpocketing.

These perspectives are intrinsically different and, depending on the context, will therefore result in different statements about the relevance of a behaviour to security. The same behaviour can differ from one perspective to another: it may be normal in the one and deviant in the other. The classification of a behaviour as “deviant” according to one or more of these definitions does not necessarily imply that the behaviour is also “bad”.

The conditions for using these perspectives, and their usefulness, differ. For example, if there is a tangible and specific threat, one may allow oneself to examine behaviour that is associated with a particular modus operandi. If there is a general elevated threat level but no information about the nature of a specific threat, it may make sense to examine all deviations of the normal operating processes. In all cases, also in the event of low threat and low readiness, one can opt to incorporate stimuli to be proactive, combined with being wary of the modus operandi of prevalent crimes.

Deviations of social standards and the fulfilment of (negative) stereotypes is generally unlikely to generate information about a tangible threat unless there is information in advance about the social identity (like culture) of an individual, causing these perspectives to quickly lead to discrimination on the basis of social background. In situations where the threat is very high and no alternatives exist, such aspects may be examined to at least get an information position, such as a normal picture of social behaviour. But this will easily lead to errors and controversies if biases like *surveillance bias* and *exclusion bias* occur.

Independent of the chosen perspectives, it is rare for a single deviation in behaviour to raise suspicion. This is more often generated by a series of subtle deviations [27] (Dutch).

5.2 Methods for determining deviant behaviour

The nine perspectives of deviant behaviour above are not specific enough for operational supervisors. There are various sources and methods that help further specify deviant behaviour. We have compiled the list below on the basis of a literature study, interviews and experiences in projects. Most of them have already been used previously in various projects on deviant behaviour. All the methods use one or more information sources such as literature, the experience of people or direct observation at surveillance locations. [21] considers several methods:

- Questionnaire or interviews with experts;
- Analysis of the state of the art of automated systems;
- Eyeball-tracking and verbal communication between CCTV operators;
- Verbal report by CCTV operators;
- Literature study;
- Direct observation;
- Grounded theory;
- Morphological analysis.

This is by no means a comprehensive list; the last two methods are new in the context of deviant behaviour and their use is introduced in this report. Other methods may be developed and this list may already be incomplete.

The methods are sometimes interdependent. For instance, the premise for direct observation is an initial rough notion of what aspects could be relevant, and may well emanate from the grounded theory method or morphological analysis. Direct observation can subsequently confirm or negate any ambiguous findings from other methods.

The methods are compared with each other in terms of a number of dimensions proposed by the Scientific Council for Government Policy in its report ‘iOverheid’ (iGovernment) [26], including the dimensions *freedom of choice, privacy*, and *effectiveness* (=*security* in this context). A key step in determining effectiveness is the empirical validation of the predictive value of behaviours in practice.

Based on the list of characteristics per method, the efficiency of these methods appear less appropriate for the process-based principles like traceability and transparency, partly because these aspects put additional demands on the data-gathering and storage that underlie the methods. So, opting for a balance as a metaphor, as the WRR does, is correct in that sense. However, there are methods that perform better “on average” although some components are also worse. In the final sections of chapter 3 of the original Dutch report [22] two composite methods are presented that compensate for the weaknesses of individual methods and can be made specific to the circumstances.

6 Observation of deviant behaviour

From a security and surveillance point of view, observability is the degree to which something can be observed by another than the subject itself. ‘Observable’ is a complex notion that technological advancements have made increasingly wide. In 2009, for instance, the detection of a person’s heart rate from a distance was not considered observable [14] whereas the use of normal webcams made this possible just two years later [19]. In another example Bouma describes how today behaviour can even be automatically observed so that it is predictive for pickpocketing [2]. Observability is influenced by all kinds of factors, including the characteristics of the observer, the maximum accepted invasiveness and circumstances such as the weather, complexity of the scene, etc.

The intention of people to commit a crime, before the crime has happened, is a valuable piece of information for proactive security. However, intention itself has not yet been directly observable in practice; various related physiological elements can be observed or even measured but these are only indirectly indicative of intention. People can also be asked about their intention but they can lie and are likely to do so if that favours them. Estimating someone’s intention therefor always involves a significant degree of uncertainty.

6.1 Surveillance patterns

In [23] a set of *surveillance patterns* were introduced: general reusable solutions to commonly occurring surveillance challenges. They have in common that they take data as input (situational awareness), and generate alarms as output (threat assessment). Five surveillance patterns have been identified: threshold alarm, profiling, concentric circles of protection, bag of words and scenario view. They can be employed by humans and machines alike.

The surveillance pattern *profiling* is of a fundamentally different nature then the other surveillance patterns because it is just an assumption based on statistics, and not an observation, let alone a measurement, as the other patterns are. The next section discusses profiling and specifically *predictive behaviour profiling*.

6.2 Profiling

Profiling is an extrapolation of a characteristic of a person, a group or a situation on the basis of other characteristics of the respective subject. Profiling neither measures nor observes; it is a statistically founded assumption and can therefore never be used as evidence or to give weight to other evidence [9]. For example, if profiling (of groups) is used in riot control to decide upon the use of violence, both the chance and the impact of errors in judgement are increased .

Profiling can be characterised in various ways, on the basis of time in relation to the incident, input or output variables, object of profiling and application domain. Chart 4 provides a list with examples.

Chart 4 Profiling characterisations.

Profiling characterisation	**Examples**	**Descriptions**
Pre or post incident	Predictive profiling	Ascertain the possibility of someone becoming involved in a future incident (as offender).
	Offender profiling; Criminal profiling	Ascertain the possibility of someone having become involved in an actual incident (as offender). Vice versa draw up a profile of the offender.
Input of profiling	Behavioural profiling	Ascertain an aspect of a person (such as his intention) on the basis of his behaviour.
	Racial profiling	Ascertain an aspect of a person on the basis of his race.
Output of profiling	Geographic profiling	Ascertain a person’s residence or place of work on the basis of other aspects.
Domain	Cybercrime profiling	Profiling people or situations in order to prevent or solve cybercrime.
Object of profiling	Person	Profiling people.
	Group	Profiling groups of people in crowds.
	Situation	Determining whether a situation is suspicious.

6.2.1 Effectiveness of predictive profiling

Effectiveness is the capability to produce a desired effect. In security, desired effects are typically the prevention, disturbance or resolution of a crime. Since profiling is only a means to such ends, a measure of effectiveness of profiling should in principle be determined as the (traditional) measure effectiveness of a process that utilizes profiling to create an effect in the real world, e.g. investigation (cases solved), access control (caught intruders) or the security check at an airport (caught people carrying weapons). For example, the effectiveness of forensic geographic profiling is the contribution to the capability to solve cases. This makes attributing effects to profiling difficult: was an effect caused by profiling, or by another part of the security process?

If the effectiveness of only a sub process (e.g. surveillance) or subcomponent (e.g. a trained profiler) of a security system is to be determined, the definition of a measure of effectiveness should be expressed in terms of the function of the particular sub process or component, i.e. the effect it has on creating situational awareness or threat assessment. In this case, the effectiveness of profiling is the capability to assess the desired variable of the object of profiling. For example, the effectiveness of geographic profiling is the capability to assess a geographical attribute of the object of profiling, e.g. his place of birth, place of residence or place of work, or a combination thereof.

Predictive profiling is typically used to create an effect either before the incident occurs, e.g. prevention (including deterrence) or during an incident, e.g. disturbance and catching someone in the act. The effectiveness of profiling during an incident is therefore the capability to disturb, or the capability to catch someone in the act.

If predictive profiling is used to create an effect before an incident, there are four factors which make the definition of a measure of effectiveness problematic. First, because it is impossible to proof the presence or absence of a future event. Second, because it is unethical to not intervene to find out if a crime is actually committed if you already have a reasonable suspicion. Third, because predictive profiling is typically based on assessing the current state of a hidden attribute –e.g. intent- which with more or less accuracy predicts or even causes a future event. Since such attributes cannot (yet) be defined as a physical quantity, they cannot be measured. And fourth and finally, people can lie about their intentions, especially if they have bad intentions.

Therefore, a less direct way of defining the effectiveness of predictive profiling is necessary, which was already introduced in section 2. We propose therefore to use the capability to frustrate or stop the transition through criminal phases as measure of effectiveness for predictive profiling, in fact as a measure of effectiveness for any (proactive) security measure. The effectiveness of predictive profiling in counter terrorism can therefore be e.g. the capability to prevent people to transfer from “broad target selection” to “specific target selection”. This does create new challenges. How do you know how many people are currently in a particular phase before the crime? For serious crimes such as terrorism, it is a purpose of the intelligence process to monitor the process from radicalization to executing an attack. Another approach is to look at phase-specific effects. An effect on the broad target selection phase is e.g. the displacement of crime. So, the displacement of crime is a desirable measure of effectiveness of proactive security, at least from a security point of view.

6.2.2 Predictive behavioural profiling using prodding actions

Prodding actions as a surveillance method are used for the predictive behavioural profiling of people. It is a form of behaviour profiling because a statistical assessment is made of a variable (as of yet non-measurable) of a person: e.g. the intent of a person to do something dangerous. Prodding consists of the active variation of stimuli on one or more persons, without which it can take a long time before enough information is gathered about a person to be able to state anything useful about his intent. This active prodding in an environment and context as selected or designed by the supervisor, shortens the time window of the necessary surveillance. It thus enables more specific information to be derived and, therefore, increases both effectiveness and efficiency. Stimuli are by definition invasive. In theory, the entire spectrum of invasiveness is possible. In practice, surveillance in public spaces tends to vary up to level 6: *interrupt*. *Security questioning* is a form of prodding actions.

A good stimulus – from a surveillance perspective – is *distinctive* in that people with a (certain) bad intention will react significantly differently to people with a (certain) good intention. A stimulus to which both react in the same way is not helpful, therefore. A good stimulus thus leads to perceptibly different reactions.

In this *Deviant Behaviour* research programme, Wijn and colleagues have studied the efficacy of stimulation in controlled conditions. This revealed, among other things, that stimulation leads to a better assessment of whether people under high(er) mental pressure have bad intentions [27].

If prodding is used for predictive behavioural profiling, then the effectiveness of prodding in itself is the extent to which, for instance, the intention can be determined. But, prodding is a relatively new instrument for which no harmonised effectiveness or quality yardsticks have been developed yet. Therefor it is recommended to develop such yardsticks in a European context and use them on the training courses on offer.

The effectiveness of training in prodding in a wider context, however, must be expressed in terms of the goal of the training, such as the detection (and deterrence) of people bearing arms at a flight security checkpoint. In such a case prodding may generate a lot of by-catch, as the prodding actions must be designed to be specific for taking weapons aboard an aircraft. The next paragraph discusses the case of SPOT of the TSA in the USA.

6.2.3 TSA and Screening of Passengers by Observation Techniques (SPOT)

The Transport Security Agency (TSA) uses the Screening of Passengers by Observation Techniques (SPOT) programme to check passengers at airports prior to boarding. The SPOT programme works by training Behaviour Detection Officers (BDO's) in observation of behaviour and appears to focus on the detection of lies and deception [5]. This is just one aspect of stimulation. The suggestion in the restricted public information that a list of behaviours is being studied, without reference to the associated stimuli, also suggests that a very specific approach has been adopted. The SPOT programme can thus not be regarded as representative of the Dutch situation, although there are lessons to be learned from evaluations of this programme.

One of the key lessons concerns efficacy and effectiveness of the programme. There is no public data on the efficacy, and the Governmental Accounting Office of the United States also claims that there is no information on the effectiveness [17], thereby advising that the programme be paused until there is such information available.

6.3 Describing deviant behaviour

To be able to determine behaviour, and communicate about it, behaviour must be described clearly and simply. This section describes the *modus operandi map*, which is developed for human use. The second part of section covers the lack of suitable formal (technical) metadata schemes for surveillance in general.

6.3.1 Modus operandi map

The modus operandi map is a way of recording a behaviour succinctly. The MOMAP can help gain rapid insight into the variation of modi operandi within a type of crime, and is particularly suited in combination with the morphological analysis and the *grounded theory* methods. These methods and aids may well turn out to be useful for the analysis of both crimes and normal behaviour.

The usefulness and efficacy of the MOMAP as a means of communication has been qualitatively validated on a small scale by operators. It is recommended to continue the development of a standardised method of communicating about (deviant) behaviour, including its validation among professionals.

Chart 5 MOMAP of pickpocketing on a tram platform with pickpockets working together.

MOMAP Pickpocket							
In the pickpocket scenario generally two or more (two is common) pickpockets work together. They are usually opportunistic criminals, selecting victims based on their vulnerability and likelihood that they carry cash.							
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*	*10:37*	*10:37*	*10:37*	*10:38*
Persons 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 cash 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 set in scene by the Amsterdam police with actors.*						

Using MOMAPs and other instruments can enable a modus operandi to be specifically described at tactical level. Developments in a modus operandi can be quickly and effectively described and communicated and thus enable better countermeasures against (new) criminality.

A number of factors played a role in opting for the pickpocketing case in this report, one of which is *recognisability*: as many stakeholders as possible have to be familiar with the case in order to be able to place the results in their context. Pickpocketing is a common phenomenon and is a regular feature in television programmes like Crimewatch or Most Wanted. Pickpocketing was also selected because the information about the modus operandi of pickpocketing is not confidential, which means that this can remain a public report and the knowledge can also be used in other research programmes that are of a more confidential nature.

6.3.2 Metadata schemes

Current metadata schemes do not address all requirements that surveillance puts on them. So, a harmonisation of metadata schemes is required. MPEG-7 may be the metadata scheme on which this harmonised approach could be built [23].

Metadata may contain very detailed personal data. A verbal transcript of a telephone conversation with the names of both conversation partners is an example of metadata. This does not correspond with the actual use of this term in the media and by some government organisations where the term metadata is used to indicate that the contents of a telephone conversation are *not* recorded. This much more restricted interpretation of metadata may lead to misunderstandings among the various communities of policy, science, privacy, technology, politics and security.

6.4 Technological support and developments

Knowledge about statistically deviant behaviour can help determine which behaviour combinations are actually indicative in a certain environment and context of undesirable situations and may even be predictive of behaviour for some forms of criminality. System developers can subsequently make technically better detectors for certain behaviours since they can use this knowledge to know specifically which behaviours are relevant or not. For example, Bouma describes how behaviour that is indicative of pickpocketing can be automatically detected [2].

6.4.1 Observing deviant behaviour with CCTV

Observability of humans in general by using surveillance cameras is described by a rule of thumb which distinguishes monitoring, detecting, observing, recognising and identifying [12]. Such rules of thumb are important since they can be an efficient way of achieving effective surveillance, although they must not lead to *law of the instrument* bias. This particular rule however is outdated. No account is taken of variations in resolution in images, variation in user interfaces (e.g. mobile devices) or the vast diversity in human behaviour, and there is no account of other surveillance resources than cameras. It is recommended to describe and validate a new rule of thumb for the observation of deviant behaviour. E.g. which is related to invasiveness and/ or specific modi operandi.

6.5 Societal values in the design of surveillance systems

Human values such as liberty and privacy need to be reflected in the design of surveillance systems, preferably in a methodological manner. This involves the mitigation of biases, and the protection of privacy and personal data.

6.5.1 Mitigating biases

The incidence of biases is a real risk in observing and in registering observations: *confirmation bias*, *exclusion bias* and *surveillance bias* are just a few examples of possible distortions in the overview. By recognising, realising and, as far as possible, proactively mitigating these biases, errors can be prevented. The supervisor himself can more objectively assess situations and this knowledge allows him to be more conscious of what one sees and makes of this. The implicit knowledge in the heads of supervisors is also made explicit and can also be validated by unbiased observations. Preventing biases is also essential for the support of security measures by surveillance subjects and society.

Taking a poll of operational supervising personnel provides insight into why they act as they do. For instance, what views of deviant behaviour are used, and what knowledge do they have of the modi operandi of prevailing crimes. From this it may be derived whether prejudice or biases are likely to occur. An example may be ascribing a type of pickpocketing to a particular nationality (such as a Romanian method of pickpocketing, a Bulgarian burglary manner or an Italian type of bag snatching) whereby the possibility of biases may increase. Early in this study ideas about deviant behaviour were checked among professional supervisors, in part via a questionnaire, but the questions lacked the focus to generate such insights. It is therefore recommended to develop a (standardised) questionnaire to be able to warn at an early stage where biases are developing among supervisors, or at least to continue to create relevant awareness.

6.5.2 Privacy-by-design for proactive surveillance

Organisations that wish to use new technology and methods have the responsibility of not unnecessarily encroaching on privacy. Privacy by design can help identify and prevent such risks early on. However, the concept is still under development [24]. Specifically privacy by design for security systems, and especially for behaviour profiling systems, is still in its infancy. For this reason it is recommended to develop privacy by design for security systems in a European context.

7 Conclusion

Deviant behaviour recognition is used both before, during and after an incident. However, the business case will improve the sooner an effective intervention occurs in the incident.

The key recommendation of this report is to stimulate the development of specific, empirically-based effectiveness measures and get them employed in proactive surveillance methods. Effective validation requires common and correct definitions as well as a methodical approach, something to which this report pays extensive heed. Attention is also given to principles such as effectiveness, efficiency, transparency and accountability.

All in all, on the basis of clear terminology, a methodical approach and validation in practice, it is quite feasible to arrive at specific descriptions of deviant behaviour in a certain environment (location) and context (threat and vulnerability). The enforcing authority can communicate to the public about the prevailing views of deviant behaviour and how these are translated into concrete behaviours that need looking out for. The specification of stimuli and behaviours is then presented only to the supervisory bodies, which prevents the security becoming an issue since the concrete descriptions of deviant behaviour are not public.

This results in supervisors being able to use this knowledge to better observe, understand and influence human behaviour while maintaining the human dimension.

8 Literature

[1] Baron, J. (2007). Thinking and deciding (4th ed.). New York, NY: Cambridge University Press.

[2] Bouma, H. et al, (2014) *Automatic detection of suspicious behavior of pickpockets with track-based features in a shopping mall*, Proc. SPIE, vol. 9253, (2014), accepted for submission

[3] Burgoon, J.K., Blair, J.P., & Strom, R.E. (2008). Cognitive biases and nonverbal cue availability in deception detection. Human Communication Research, 34, 572–599

[4] Burgoon, Judee K., et al. "Maintaining and restoring privacy through communication in different types of relationships." Journal of Social and Personal Relationships 6.2 (1989): 131-158.

[5] Department of Homeland Security Office of Inspector General, Transportation Security Administration's Screening of Passengers by Observation Techniques (2013)

[6] Devine, P.G. (1989). Stereotypes and prejudice: their automatic and controlled components. Journal of Personality and Social Psychology, 56, 5-18.

[7] Farrington, David P., Brandon C. Welsh, and Doris Layton MacKenzie. Evidence-based crime prevention. London: Routledge, 2002

[8] Gill, Martin, and Angela Spriggs. Assessing the impact of CCTV. London: Home Office Research, Development and Statistics Directorate, 2005

[9] Godwin, Grover Maurice, ed. Criminal psychology and forensic technology: A collaborative approach to effective profiling. CRC Press, 2010

[10] Gutwirth, Serge. Privacy and the information age. Rowman & Littlefield, 2002.

[11] Gutwirth, Serge, and Mireille Hildebrandt. Some caveats on profiling. Springer Netherlands, 2010.

[12] Home Office (2009), CCTV Operational Requirements Manual 2009 (28-09)

[13] Langheinrich, Privacy by design—principles of privacy-aware ubiquitous systems, UbiComp2001 (2001)

[14] Lousberg, M., et al. "Monitoring van afwijkend gedrag." Soesterberg: TNO Human Factors (2009)

[15] Lum, Cynthia, Christopher S. Koper, and Cody W. Telep. "The evidence-based policing matrix." Journal of Experimental Criminology 7.1 (2011): 3-26

[16] Lyon, David. Surveillance studies: An overview. Polity, 2007.

[17] Office of Inspector General (2013), Transport Security Agency's Screening of Passengers by Observation Techniques

[18] Oswald, Margit E., and Stefan Grosjean. "4 Confirmation bias." Cognitive illusions: A handbook on fallacies and biases in thinking, judgement and memory (2004): 79

[19] Poh, Ming-Zher, Daniel J. McDuff, and Rosalind W. Picard. "Advancements in noncontact, multiparameter physiological measurements using a webcam." Biomedical Engineering, IEEE Transactions on 58.1 (2011): 7-11

[20] Reicher, Steve D. "'The Battle of Westminster': developing the social identity model of crowd behaviour in order to explain the initiation and development of collective conflict." European Journal of Social Psychology 26.1 (1996): 115-134.

[21] TACTICS Consortium, D3.1 *Conceptual Solution Description*, 2013, http://www.fp7-tactics.eu/

[22] Van Rest, J., Roelofs, M., van Nunen, A. (2014) *Afwijkend gedrag, Maatschappelijk verantwoord waarnemen van gedrag in context van veiligheid – tweede herziene druk*, (*Deviant behaviour - Socially accepted observation of behaviour for security*) TNO Report R10425 (Dutch)

[23] van Rest, J., Grootjen, F. A., Grootjen, M., Wijn, R., Aarts, O., Roelofs, M. L., ... & Kraaij, W. (2013a). Requirements for multimedia metadata schemes in surveillance applications for security. Multimedia Tools and Applications, 1-26

[24] van Rest, J. et al (2013b), Designing Privacy by Design. In: Annual Privacy Forum 2012. *Lecture Notes in computer science*, Springer (to be published)

[25] van Rest, J., *Using Deviant Behaviour in Your Concept of Operations*, Presentation at ASIS Europe 2014

[26] W. R. R. (2011). IOverheid (p. 288). Amsterdam University Press

[27] Wijn, R., Van Rest, J. H. C., Lousberg, M., & Burghouts, G. J. (2012). Naar een beter begrip van afwijkend gedrag: Herkenning door mens en computer. In: E.R. Muller (Ed.), Veiligheid: Veiligheid en Veiligheidsbeleid in Nederland (565-587). Kluwer, Deventer

[28] Wijn, R. et al (2014), *Telling friend from foe: Environmental cues improve recognition of individuals with hostile intentions*, submitted