SIAM
Security Impact Assessment Measures

WP 3

Impact analysis on criminal actions

Deliverable D 3.1
Local Security Technology effectiveness report

Centre for
Technology and Society
Technische Universität Berlin

Dr. Leon Hempel
Lars Ostermeier
Dagny Vedder
Tobias Schaaf

Project number
261826

Call (part) identifier
FP7-Security-2010-1

Funding scheme
Collaborative Project

Table of contents

Summary

The analysis in this report has brought up some of the amibiguities at play when it comes to reporting frequently occuring and dangerous criminal actions and evaluating the impact of security technologies on security. Frequently ocurring criminal actions like theft do not necessarily spark the introduction of new security technologies. The latter requires the construction of dangerousness of criminal actions that involves changes in a certain context/space, where resources are being contested and where public imaginations of dangerousness come into play, creating a demand for an altered way of policing. Technology is often a quick answer in such a case. Assessing the impact of security technologies on security raises questions about how security is understood and how technologies are thought to relate to security. Three different ways of managing this area of ambiguity have been analysed. In the first case, security is a contested concept and the impact of a technology on security remains vague. In the second case, security has been defined as an 'adequate' problem and the impact of a technology can be 'clearly' assessed. In the third case, a security problem is being constructed in order to provide a use-case for a technological solution. This analysis provides important starting points for the development of a methodology to assess the impact of security technologies on security. The methodology will require the stakeholders to reflect and understand how a certain way of assessing the impact of a technology on security has become dominant. This involves both the consideration “of the adequacy of the approaches offered, and their ability to inform practical matters.“ (Rappert 2001: 562)

1. Introduction

1.1 Objectives

The objective of the report is to gain a first-hand understanding of what frequent and/or dangerous criminal actions are at the case study sites and how the impact of SMTs on these criminal actions is being assessed. Based on these findings, assessment criteria, attributes and questions for the Assessment Support Tool are summarised in a table as an annex to the report.

1.2 Methods

The findings of the report are based on three in-depth interviews with federal and local police and a security research expert. One interview has been recorded and two have been protocolled because the interviewees did not consent to being recorded. Requests for interviews with three other stakeholders have been rejected because they considered the topic too sensitive. For the same reason, a workshop had to be cancelled. From 10 invitations for the workshop, only one inviation had been accepted even after follow-up calls had been made. Due to the lack of interview data, the report draws on some relevant literature in order to substantiate the line of reasoning. The data has been analysed using the uniform guidelines sent out by the work package leader for work package 3 case study reports. The guidelines pre-defined the structure of the report. The results will be further elaborated in the final synthesis report of work package 3. All partners are engaged in efforts to deliver more interview material for the synthesis report.

2. Findings

2.1 Frequent and dangerous criminal actions

The perception of frequently occurring and/or dangerous criminal actions largely depends on the institutional occupancy of the interviewees. It depends on the resposibilities that their institution has been assigned with, the actions taken, the area of responsibility, and the specific legal obligations in that area of the airport how they put their answers to this question.

Frequentently registered criminal actions

- Carrying forbidden goods (defined by Aviation Security Law)

- Carrying forbidden goods (defined by customs regulations)
- Violations of immigration law
- Carrying unconventional exploding / fire devices
- Theft
- Threats to commit violent acts or to kidnap passengers or staff
- Unidentified Luggage

The Aviation Security Law (Luftsicherheitsgesetz) lists a number of aviation specific criminal actions that are to be prevented and prosecuted if detected. Among the most prominent serious crimes listed in the legislation is the hijacking of planes (see Richter 2007: 218). Another serious crime is sabotage of aircraft and airports. Here a further specification of the crime is made: (a) destroying, damage or remove installations or aircraft; (b) create obstrcuctions to civil aviation; (c) give wrong singnals or signs; (d) other dangerous interferences.

Further crimes mentioned in the Aviation Security Law are carrying of dangerous artifacts aboard aircraft or other security sensitive areas; ignoring or resisting with violence the orders and instructions of pilots and other authorities; transport dangerous goods without authorization; carrying dangerous goods without authorization; using certain electronic devices; violating closed airspace. Richter mentions that in 2006 in Germany a total of 742.342 dangerous goods have been confiscated at airports (Richter 2007: 231).

Minor breaches of the law are: giving wrong information in the process of security screening; not providing an aviation security plan; failure to implement security measures; misuse security identification cards; violating operational instructions; ignoring the orders of pilots.

Why do they occur frequently?

Airports have been described as standing in the focus of international organised crime. Furthermore, they are being considered as premium targets for international terrorism in risk assessments. Finally they create opportunity structures, especially for theft because of the large number of people travelling and the large amount of luggage and cargo. At international airports, cross-border crimes are frequently being recoreded because of the border control measures.

What are the most dangerous criminal actions?

While all of the abovementioned criminal actions can be committed at airports, it is difficult to say objectively which of them are “most” dangerous. A common way of determining the dangerousness of criminal actions is to assess the damage they can create. Following this logic, threats to commit violent acts or to kidnap passengers or staff and carrying unconventional exploding / fire devices have been described as the “most” dangerous criminal actions.

What makes these actions dangerous?

A very obvious response to this question seems to be typical: criminal actions are being considered as dangerous depending on their destructive impact on individuals and infrastructures. The construction of dangerousness tacitly implies the construction of harmless criminal actions, too (e.g. pickpocketing). One expert emphasized that this rationality is often replaced by a more complex process of the construction of dangerousness. He said that dangerousness is not necessarily tied to an empirically observable destructive impact. Rather it is the result of a process where changes in a certain context/space occur, where resources are being contested and where public imaginations of dangerousness come into play, creating a demand for an altered way of policing. Technology is a quick answer in such a case. One example for this is are spectacular violent crimes that spark a moral panic (Cohen 1972): “Dangers exist only where they are perceived as such and where they are named as such” (Interview with security expert). A problem here is that while the discourse often speaks about dangers, what is meant here are risks. Sometimes new technologies can even lead to the deconstruction of dangerousness. The TSA for example has decided to put small knives from the list of banned artifacts after a review of risk assessments. At the same time, liquid scanners are becoming operational at TSA checkpoints, rendering liquids potentially more dangerous than before.[1]

2.2 SMTs

What kind of SMTs are being operated to deal with these criminal actions?

Targeted SMTs like liquid scanner or other detection devices are mainly connected to airport specific criminal actions, while general security technologies like CCTV are used for different, more vaguely defined purposes.

[1] http://blog.tsa.gov/2013/03/small-pocket-knives-more-support-than.html

The technologies that have been mentioned in the interviews are:

- Devices to trace the origins of calls in the case of threats or kidnappings
- HD-Video surveillance systems for surveillance and recording
- Automated search databases
- Border control technologies
  - Finger print scanners
  - biometric scanners
  - Document scanners
- X-ray scanners for bord luggage and drop-off luggage
- Special technologies to identify and deal with unconventional exploding / fire devices
- Biometric access control systems
- Perimeter protection
- Security Control Center

Are there any major technological innovations that have been introduced?

The innovations mentioned in the interviews are:

- Biometric access control systems
- Automated perimeter protection
- HD video surveillance

Are any technological innovations expected that will enhance the possibility to deal with them?

Three major innovations are expected to be implemented in the coming years:

1. Automated border checks based on biometrics
2. Body-scanners for passengers and employee control
3. CCTV management systems and intelligent recognition technologies

2.3 Impact of SMTs on criminal actions

In which way have the SMTs contributed to security, and are there different dimensions of security affected?

It is difficult to say that every technology can be assessed regarding its impact on a specific criminal action. In most cases, the impact is rather assessed in terms of its

general contribution to increase 'security'. Security technologies are always a part of security measures. Interviewees argued that security technologies contribute to security through the role they play in security measures. This points out that security technologies need to be assessed in the context where they become part of security measures.[2] How this is done can be described drawing on the various dimensions of security that are referred to when the interviewees are asked to describe how SMTs contribute to security. Some examples for the impact of security technologies as parts of security measures on criminal actions that have been given by the interviewees inlcude:

- The violation of immigration laws can be countered by using finger print scanners. This example referred to the use of the EURODAC database in the Schengen border system.
- Fake passports can be detected through biometric border controls, increasing border security.
- Improved scanning technologies like the body- and liquid scanner improve the capability to detect forbidden artefacts, increasing the security by reducing the possiblity to carry dangerous artifacts into aircraft or other security sensitive areas.

These examples show that each of the assessments involves ideas about what the security problem is and the proper ways to deal with them. The dimensions of security that are impacted upon by security technologies therefore need to be made explicit by the actors in the course of the assessment processes. It is a matter of empirical investigation rather than the inclusion of abstract knowledge.[3] For analytic purposes some of the dimensions can be deducted from the abovementioned examples. One dimension of security is the definition of the role of the actors in producing security. It is obvious that the examples have been given in interviews with police staff, who in the context of German aviation security typically describe the official role of their institution as the prevention of hazards for passengers, employees and the infrastructure and border control. Another dimension referred to in the example is technological functionality: if a scanner is capable of detecting forbidden liquids, it contributes to more secure control procedures. A third dimension are the tacit assumptions about sources for insecurity. The examples mention fake passports and the crossing of borders without proper documents as causes for “insecurity”, which

[2] For example, see Manning (2008) for an ethnographic analysis of the impact of crime mapping technologies and crime analysis on policing in North American cities.

[3] Tilley (2013) has defined 12 contextual dimensions of the contribution of covert operations to security for this purpose: Motifs, Problems, Aim, Beneficiaries, Temporal Interest, Person focus, Person Question, Incident Focus, Sources, Key actors, Method, Model.

implies that measures countering fake passports and illegal border crossing increases security. In this case, security technologies reiterate existing and institutionalised organisational and political assumptions.

What is the impact of SMTs on crime?

Work package 7 of the SIAM project has brought up the thesis that three logics of security measures can frequently be observed in the context of airport and public transport security: prevention, disruption and detection. Prevention comprises both deterrence in the sense that criminal actions are not undertaken because of the risk of being detected and disrupted and measures that limit the impact of a criminal action that has been committed. Disruption often is the result of police investigations, but it can also occur by accident. It can have a preventive effect in the sense that further harm and/or damage to individuals and/or infrastructure is stopped. Finally Detection is often the result of routine controls and patrols, based on occupational models of risk and threat thinking. It is, among others, through these logics that security technologies are being mobilised in the context of security measures aiming to create and impact on crime. The three logics create different ways of constructing suspicion and dangerousness, which has an influence on how the impact of SMTs on crime can be thought.

How is the impact being assessed / measured?

Three ways of constrcucting an assessment / measurement of SMTs on criminal actions can be distinguished. The first is a conflictual way where the understanding of the criminal actions that are supposed to be impacted on is unclear or to broad, leading to generalized assumptions about the impact on these vaguely defined targets. A second way is to clearly define a criminal action that is supposed to be prevented, disrupted or detected and then to assess the success drawing on statistical findings, on intelligence or on a increase in perceived security. A third way is the determination of a criminal actions that are supposed to be prevented, disrupted or detected by technological functionalities. In this case, there is a technological problem to be solved in the first place and the criminal action that it is supposed to counter is the “use case” that has been identified in the course of the development process. Three questions summarise these different ways of assessing:

1. *Is there a problem at all?*
2. *Are we responding to an 'adequate' problem with technologies and then determine the success of the response?*
3. *Are we constructing a problem in order to solve a technological problem?*

One of the experts emphasized that there are few reliable studies showing how the use of technology X with the objective to impact on Y has been successful and is therefore legitimate. Rather the creation of such lines of argumentation frequently involves a “massive construction” where causalities are being created ex-post. Analysing this construction can reveal how different organisations and actors involved in the assessment define criteria according to their interests. Therefore there are no assessments taking place in an absolute vacuum.

A further reaching problem that has been mentioned in this context is the relationship of situated practices and rationality in security technology assessments. This relationship links the official discourse and public statements about security production with the messy reality 'behind the scenes'. It captures the observation that the analysed rationales are attempts to make the unforseeable accessible to rational planning. Security planning thus alwayse involves a refocussing of the gaze on the unforseeable. Making visible this relationship could be a good starting point to develop a method/model for security technology impact assessment in SIAM.

Another, closely related aspect is the question for more adequate/alternative rationales. A famous approach in this line of thinking is the random use of SMTs for security production, creating a security environment where it is unclear for passengers which security measures they have to expect. This approach can be observed at Ben Gurion Airport for example.

Drawing on Rappert's analysis of non-lethal weapon assessments, one could understand the three questions analysed above as different strategies to cope with the ambiguities of security technologies. It is these processes that need to be made more explicit through the SIAM assessment tool. Some of these ambiguities named by the security expert include:

- How do security technologies and security measures change the social space and what are the consequences of the change?
- How do the different mechanims of a security measure interact?
- How do the actors interact and how do they negotiate different interests and objectives?
- What is the role of cultural factors in the negotiaton / assessment process?

The result of the negotiation of the ambiguity of security technologies is what can be called a 'control culture', that is a local product of the stakeholders involved in producing security.[4]

[4] For the notion 'control culture', see Ostermeier 2008; for the further-reaching notion 'security culture' see Daase et al 2012.

However, in the public discourse the most frequently invoked strategy is the one where it is presupposed that security measures are responding to an adequate securtiy problem and the impact on this problem is being measured. The police inteviewees offered two ways of assessing the impact following this logic. One is to use statistical evidence and police intelligence to assess the impact. The other is to ascribe an increase of the clearance rate to the succesfull implementation of security measures.

When is an SMT considered ineffective?

Interestingly, ineffectiveness seems to be the result of the same complex processes that lead to the rendering of a technology as effective. Interviewees said that to be effective, a technology needs to 'fit' in the security measure. In other words, it is ineffective if it does not fit. What this means, varies from case to case. It can mean that it disturbs organisational routines, that it has a high false-negative rate, that it does create unforeseen costs, that it does tower above the space that is available in a certain setting or that it creates protests from users or passengers.

How do notions of crime and security change in the course of the introduction of SMTs?

One interviewee said he observed how the 'appearance' of a criminal action changed after a technology had been introduced, leading the criminals to adapt the way they commit crime and increasing the risk to be discovered. Again, it needs to be reconstructed from case to case how crime patterns[5], comprising imaginations of criminals and of opportunity structures, have played into the decision to introduce a security technology and to evaluate its contribution to security. Close attention needs to be payed to how the crime patterns are being constructed and how criminals react to these patterns. This leads to a situation where criminals adapt their behavior to crime patterns, following a pattern of 'reciprocal anticipation'. Reciprocal anticipation might provide a starting point to investigate deeper how notions of crime and security change in the course of the introduction of SMTs.

Which unintended consequences have been observed after the implementation of the specific SMT?

- *Unintended Consequences on criminal actions*

As already indicated in the previous paragraph, a focus on rational planning models might lead to the creation of new vulnerabilites, which is an unintended consequence of a security technology.

[5] See work package 7 reports.

- *Unintended Consequences on freedoms*

It is disputed in the academic discourse whether targeted measures relying on rational planning models or random measures are better suited to avoid unintended consequences on freedoms. What is important to note is that according to Rappert's (2001) line of reasoning, a technology itself can never be designed in a way that it cannot be used to infringe freedoms. What avoids freedom infringements is the way how technologies are deployed (that is, the security measures).

- *Unintended Consequences on organizational routines (function creep)*

The interviewees did not elaborate on unintended consequences on organizational routines.

To what extent have the promises of SMTs been delivered?

As it should have become clear by now, all interviewees offered a more complex picture that would not allow a simple yes or no answer to the question if the promises have been delivered. It again depends on the case that is being assessed.

3. Conclusion

Rappert's (2001) conclusion seems to be a good summary of the interim results of the analysis that is on-going in work package 3: „a fruitful line of analysis regarding the relation between technology and politics is to examine the way in which the ambiguities associated with technologies are managed, and the manner in which the distribution of amibuity helps constitute technology.“ (Rappert 2001: 559) The analysis in this report has brought up some of the amibguities at play when it comes to determine frequently occuring and dangerous criminal actions as well as the evaluation of the impact of security technologies on security.

Frequently ocurring criminal actions like theft to not necessarily spark the introduction of new security technologies. The latter requires the construction of dangerousness of criminal actions that involves changes in a certain context/space, where resources are being contested and where public imaginations of dangerousness come into play, creating a demand for an altered way of policing. Technology is often a quick answer in such a case. At the same time, it is often unclear or forgotten what the question was that has led to the answer.

Assessing the impact of security technologies on criminal actions raises questions about how security is understood and how technologies are thought to relate to security. Three ways of managing this area of ambiguity have been analysed. In the first case, security remains a contested concept and the impact of a technology on

security remains vague. In the second case, security has been defined as an 'adequate' problem and the impact of a technology can be clearly assessed. In the third case, a security problem is being constructed in order to provide a use-case for a technological solution.

This analysis provides important starting points for the development of a methodology to assess the impact of security technologies on security. The methodology will require the stakeholders to understand how a certain way of assessing the impact of a technology has become dominant. This involves both the consideration “of the adequacy of the approaches offered, and their ability to inform practical matters.“ (Rappert 2001: 562)

4. Annex

The following table is a first attempt to present the result of this report in the form of a table that is structured along the major dimensions of the SIAM assessment tool. It will be further elaborated in cooperation with the partner Kingston University in the final data integration report of work package 3.

Dimension	**Assessment Criteria**	**Attribute**	**Question**
Security	Scope	Targeted ST	Are we responding to an 'adequate' problem with technologies and then determine the success of the response?
Security	Scope	Multi-use ST	Is there a clearly defined security problem at all?
Security	Scope	Targeted ST	Are we constructing a problem in order to solve a technological problem?
Security	Planning Rationale	Prevention	Is the objective to deter or to limit the impact of a criminal action?
Security	Planning Rationale	Detection	Are there any workarounds to avoid detection?
Security	Planning Rationale	Disruption	How reliable are measures to disrupt criminal actions?

Security	Threat	Dangerousness	How has the dangerousness been constructed?
Security	Threat	Harmlesness	How has the harmlessness been constructed?
Trust	Consensus	Negotiated Consensus	How do the actors interact and how do they negotiate different interests and objectives?
Trust	Cultural Factors	Negotiated Consensus	What is the role of cultural factors in the negotiaton / assessment process?
Trust	Social impact	SMT	How do security technologies and security measures change the social space and what are the consequences of the change?
Efficiency	Reliability	Interoperability	How do the different mechanims of a security measure interact?
Freedom Infringements	Intended Infringements	Security Measure	Is the security measure proportional?
Freedom Infringements	Unintended Infringements	Security Measure	Can the security measure be altered to avoid unintended infringements?

5. References

Cohen , S. (1972), Folk Devils and Moral Panics. Oxford : Blackwell

Daase, C./Offermann, P./Rauer, V. (2012), Sicherheitskultur. Soziale und politische Folgen der Gefahrenabwehr, Frankfurt/Main: Campus

Manning, P.K. (2008), The Technology of Policing. Crime Mapping, Information Technology, and the Rationality of Crime Control. New York and London: New York University Press

Ostermeier, L. (2008), Die Polizei zwischen lokalen Kontrollkulturen und globalen Trends der Kriminalitätskontrolle, in: Kreissl, R./Ostermeier, L./Barthel, C. (Ed.): Policing in Context. Rechtliche, organisatorische und kulturelle Rahmenbedingungen polizeilichen Handelns, Berlin/Wien, 103-124

Rappert, B. (2001), The Distribution and Resolution of the Ambiguities of Technology, or Why Bobby Can't Spray, Social Studies of Science, Vol 31, No 3, 557-591

Richter, S. (2007), Luftsicherheit. Stuttgart: Borberg

Tilley, N. (2013), Intelligence-Led Policing and the Disruption of Organised Crime : Motifs, Methods and Morals, Presentation at the New Models of Expertise and Democratic Participation in Policing Conference, Centre Marc Bloch, Berlin, March 13 2013