SIAM
Security Impact Assessment Measures

Impact Analysis Report

Deliverable 3.7
Impact Analysis Report

Dr. Leon Hempel
Lars Ostermeier
Tobias Schaaf
Dagny Vedder

Project number
261826

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

Funding scheme
Collaborative Project

TABLE OF CONTENTS

1. Introduction

This report synthesises the findings of work package three (Impact analysis on criminal actions) and work package seven (Criminal actions – patterns and places) of the SIAM project. The report begins with an outline of the theoretical take on security impact assessments that has emerged in work packages three and seven and that has been used to develop the content for sections three and four of this report. The following sections are designed to achieve two objectives. The first objective is to develop guidelines for the SIAM Assessment Support Toolkit (SIAM AST, section 3). The second objective is to provide content for the SIAM database and online tool (section 4). The report is based on an analysis and synthesis of the various deliverables that have been produced in work packages three and seven as well as on an additional review of academic literature and official documents.

2. Theoretical scope: Assessing the Impact of Security Measures and Technology on Security

Impact assessments always include what can be called "the politics of knowledge production": Normative decisions about what is supposed to be known and what is supposed to be ignored or concealed and what is supposed to remain ambiguous.[1] A recent report by the United States Government Accountability Office (GAO) on the effectiveness of behaviour detection in aviation security provides for a good example how the politics of knowledge production in impact assessments work. Drawing on the observation that there is no "scientific" evidence available supporting the assumption that behaviour detection effectively contributes to reducing risks in aviation security, the GAO recommends limiting funding for security measures involving behaviour detection. However, the lack of scientific evidence is being ignored both by the Department of Homeland Security (DHS) and by the Transport Security Authority (TSA), saying that the programmes will be further enhanced to

[1] In Science and Technology Studies, the notion „ontological politics" has been used to analyse the normative and political dimensions of research and methods (see Annemari Mol (2002) *The Body Multiple: Ontology in Medical Practice*, Durham: Duke University Press). For an excellent analysis based on this literature, see: Brian Rappert (2012) *How to Look Good in a War. Justifying and Challenging State Violence*, London: Pluto Press.

increase their effectiveness.[2] This reaction on the critique towards the effectiveness of security measures has been observed in the research for this report repeatedly. It is instructive for the impact assessment of security measures and technology on security for a number of reasons.

First, it shows that despite the claims by security officials and policy makers, security policies are not rational and are not being implemented in a rational way. "Scientific" evidence and objectivism are not at the core of security activities – despite contemporary attempts to make security activities appear rational in the sense that they are "surgical" or "targeted".[3] *Second*, it shows that science is finding it difficult to rationalize the security discourse or security activities by producing "facts" because these facts are frequently being ignored. This highlights the limited role that science can play to rationalize security activities and discourses, which has consequences for the whole field of civilian "security research" of which the SIAM project is a part. Security is a slippery and contested term that relates to a complex assemblage of actors, values and activities, rendering it hard to define universally and inherently political. *Third*, this shows that the modernizing narrative coming with every security technology is fundamentally flawed. Security activities are characterised by a fetish on technological solutions for societal phenomena, effectively limiting the scope how "security problems" can be understood and approached.[4]

The latter becomes clear if one considers contemporary attempts to ban killer robots by the United Nations. Proponents of killer robots like Ronald Arkin argue that they might one day act even more ethical than human beings, saving civilian lives in greater numbers than human warriors.[5] Despite the fact that this claim will (hopefully) never become validated because of the ethical concerns that an experiment in this regard would raise, it points to a flawed understanding

---

[2] Government Accountability Office (2013) "AVIATION SECURITY: TSA Should Limit Future Funding for Behavior Detection Activities", GAO-14-159, available at http://www.gao.gov/assets/660/658923.pdf (last access 3 December 2014).

[3] Mariana Valverde and Michael S. Mopas (2004) "Insecurity and the Dream of Targeted Governance" in Wendy Larner and William Walters (eds.), *Global Governmentality*. New York: Routledge, pp. 233-250.

[4] IRISS Consortium (2012): Surveillance, fighting crime and violence (Deliverable D1.1), http://irissproject.eu/wp-content/uploads/2013/04/Surveillance-fighting-crime-and-violence-report-D1.1-IRISS.pdf (last access 15 November 2013).

[5] http://www.cc.gatech.edu/ai/robot-lab/online-publications/formalizationv35.pdf (last access 3 December 2013).

of technologies. It suggests that technologies, and not the way they are being used, can balance human failures, concealing security research's active role in altering security policies and activities. Consequently, and this is the *fourth* instructive observation, the way that technologies provide the ground for human failures by altering existing security activities or creating new ones tends to be ignored because all attention is focused on the way that the promises of the technologies can be honoured. Instead of investigating the complexities of the relationships between technologies and society, simplistic arguments are too often being taken for granted, leading to flawed decisions. This can be observed in the DHS's decision to ignore the GAO's findings as well as in the decision by the United Nations not to demand a ban of killer robots, but to ask for the establishment of an expert group that is supposed to investigate whether or not soldiers may leave the decision to kill to robots or not.[6] *Fifth*, this highlights the difficulties to regulate security activities. The whole contemporary debate about (post)privacy is emblematic for these difficulties because it shows how regulations are always lagging behind technological developments, be it legal or more informal regulations.[7] In sum, when assessing the impact of security measures and technologies on security, it needs to be considered that the impact assessment itself is a part of the security policies and activities that it aims to assess. Impact assessments, despite all the ambiguities characterising them, therefore always contribute to the production of social order.

How important it is to understand this role of security research and impact assessment in the production of order becomes clear if one analyses the reasons why security measures and technologies are being promoted. Automated video analysis at airports, for example, is being promoted because it helps to track people who at some point of the travel process have been labelled as “suspicious”. A frequently cited scenario in this regard is an incident that happened at Munich's airport.[8] There, a traveller took his laptop that had shown

[6]http://www.deutschlandfunk.de/kriegswaffen-uno-beraet-ueber-verbot-von-killerrobotern.676.de.html?dram:article_id=270541 (last access 3 December 2013)

[7] IRISS Consortium (2013) The Legal Perspective. A report presenting a review of the key features raised by legal perspectives of surveillance and democracy, http://irissproject.eu/wp-content/uploads/2013/04/Legal-perspectives-of-surveillance-and-democracy-report-D2.3-IRISS.pdf (last access 15 November 2013).

[8] http://www.theguardian.com/world/2010/jan/20/munich-airport-laptop-explosives (last access 3 December 2013)

positive traces of explosives with him and simply disappeared from the security checkpoint. This forced the police to completely shut down the airport and to clear the security area, creating hours of delays and immense costs. Note, however, that this is not a core problem for the police but for the airport and the airlines. The police have an interest in tracking third country foreigners arriving and changing planes at major hubs because it is often difficult to prove where asylum seekers have entered the European territory if they delete their travel documents. The objective, then, is not so much to reduce costs but to enhance border protection and the enforcement of immigration law. Anybody assessing the impact of automated video analytics on airport security will have to make decisions how to weigh which of the objectives: saving costs, border protection, enforcing immigration law, protection of fundamental rights. The balance metaphor often being employed in this context to dissolve the tensions has by now been acknowledged as overly simplistic.[9] It comes as little surprise that however these decisions are made, the results are frequently difficult to compare because they are dependent on the local context where an assessment is being made.[10]

These deliberatively chosen examples and their implications for security impact assessments highlight the complexity of the task to assess the impact of security measures and technologies on security. (Ir)rationality, ignorance, concealment and modernization and multiple realities are major are, to phrase it with a pragmatic term, challenges for security impact assessments. Before approaching these challenges and turning them into recommendations for security impact assessments, the theoretical scope of security impact assessments as they are being understood in this report will be briefly outlined.

The overall theoretical framework for impact assessments in SIAM is based on the innovation journey concept by Van de Ven et al.[11] This approach provides for a model of research and innovation processes, distinguishing

[9] Lucia Zedner (2005) “Securing Liberty in the Face of Terror: Reflections from Criminal Justice”, Journal of Law and Society 32 (4), pp. 507-533.

[10] Leon Hempel, Lars Ostermeier, Tobias Schaaf, and Dagny Vedder (2013) “Towards a social impact assessment of security technologies: A bottom-up approach”, Science and Public Policy 40(6), pp. 740-754.

[11] Andrew H. Van de Ven, Douglas E Polley, Raghu Garud, and Sankaran Venkataraman (2008) *The Innovation Journey*, New York: Oxford University Press.

different phases and intervention points as well as different actors and assessment criteria for each phase and intervention point. The SIAM AST is composed according to this model, providing methods for impact assessments at different phases and intervention points of the innovation journey. Drawing on social constructivism, impact assessments in SIAM are being understood as processes of knowledge production, suggesting that the realities of security measures and technologies are being enacted in impact assessment practices. In other words, in our understanding, impact assessments are always more than merely an assessment of risks or the future consequences of decisions. They are always also a part of the future consequences. It is important to consider these methodological aspects of SIAM because the SIAM provides a toolkit comprising methods for knowledge production: an online assessment tool and a number of guidelines and methods for specific topics such as security impact assessment, cultural differences, legal frameworks and freedom infringements. The normative scope of SIAM in this lies not so much in the creation of a consensus but in the creation of “productive irritations”. Productive irritations are the result of a broadened scope of the assessment by considering multiple perspectives from a large number of stakeholders and of an increased reflexivity of decision making.

Assessing the impact of security technologies faces the challenge to remain sensible for the contested nature of security definitions and at the same time to provide some guidance for approaching the question whether or not security technologies contributes to security – or even reduce it. Drawing on research that has been conducted on crime maps and security impact assessments in work packages three and seven in SIAM, this report provides a synthesis of the results. In the following sections, a contribution from work package three and seven for the SIAM Assessment Toolkit and for the online assessment systems are being presented.

3. Guideline Contribution from WP 3 and WP 7[12]

Work package seven has shown that crime maps are not simply tools representing an objective image of crime but that they are tools incorporating both previously existing data about crime and ideas how it should be dealt with.[13] Crime maps include various strands of criminological crime pattern theories and are being used as tools for the planning and allocation of resources. The different rationales point towards two questions related to the use of crime pattern analysis:

1. *In the context of urban train transport security, it provides answers to the question where resources should be allocated.*
2. *At airports, most policing resources are already available at the different security areas, so the question here is not so much on where to use them, but on how or against whom to use them.*

Different rationales of selecting and using security technologies in the contexts of urban train transport security and airport security can be distinguished and analyzed. One characteristic is the different impact of crime pattern and threat pattern analysis. It serves mainly for the identification of so-called 'hotspots', the types of crime that are recorded at these locales and a more or less vague categorization of victims and offenders in urban train transport security. In the context of airport security, threat pattern analysis typically leads to a profiling of passengers. Another major difference is the emphasis being made on passengers' perception in urban train transport security discourses, while economic considerations are being emphasized in all areas of airport security.

Both questions imply different definitions of security and different dimensions of trust, efficiency and freedom infringements. This affects the way

[12] This section draws on the deliverables that have been produced in work packages three and seven of the SIAM project.

[13] The same is true for „crime signatures“ being used in automated video analytics. „Crime Signatures“ basically resemble the idea to make crimes machine-readable in the way that threat assessments have been made machine-readable in work package 6 in SIAM. The first problem of this approach is that threats can be defined informally while crimes are defined by law. Strictly speaking, the police do not record crime but suspicious behavior probably fulfilling the legal definitions of criminal actions. Whether or not these actions are „criminal“ is being decided in courts. Crime signatures therefore always refer to „suspicious“ behavior which requires a distinction between a suspicious and a non-suspicious situation.

that the behaviour of passengers becomes normalised, the groups of people being targeted and excluded. Perhaps the most obvious difference is the basis for interventions in both rationales. In order to better understand the basis, it is helpful to distinguish between the anticipative concepts of precaution, pre-emption and preparedness and prevention. The three concepts stand for a gradual decrease of the threshold for interventions, thus bearing the potential increase of freedom infringements compared to preventive security measures. *The rationale that has been analyzed for urban train transport security can be characterised as* ***preventive****, whereas airport security increasingly becomes* ***anticipative****.*

Work package three has investigated how the effectiveness of security measures and technologies can be and is being assessed in terms of increasing security. This research has brought up the inherently political dimension of impact assessments and highlighted some of the ambiguities at play when it comes to determining frequently occurring and dangerous criminal actions as well as the evaluation of the impact of security technologies on security. Frequently occurring 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. At the same time, it is often unclear or forgotten what exactly the initial question was that has led to the answer. Assessing the impact of security measures and technologies on security often leads to the question: **Technology is the answer, but what is the question?**

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 reconstructed in work package three. 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.

Generally speaking, it is important to distinguish the rationale of the security measure from the beginning of the assessment on. For example, crime prevention does not necessarily involve the detection of crime. This is important for the assessment of the effectiveness of security measures because it appears that the detection of crime is the unlikeliest use case of security measure technologies. Rather, the likeliest use case is the detection of suspicious and possibly threatening actors, tools and activities. Much more difficult to measure, the likeliest effect in terms of prevention is the interruption and the so-called general preventive effect, which is difficult to measure.

Summarising his experience of the political dimensions of security technology assessments, Brian Rappert has suggested that

> „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 ambiguity helps constitute technology.“[14]

A methodology to assess the impact of security measures and technologies should therefore aim to understand how knowledge about the assessment is being produced and how this shapes the overall result of the assessment. This involves both the consideration “of the adequacy of the approaches offered, and their ability to inform practical matters.“[15]

Work packages three and seven have provided important requirements for the development of a methodology to assess the impact of security technologies on security. The methodology requires the stakeholders to understand how a certain way of assessing the impact of a technology is constituted and how it has become dominant. **This means to understand and critically reflect the overall security narrative that is inherent to the impact assessment, including how crime is being imagined.** The narratives to be

[14] Brian Rappert (2001) „The Distribution and Resolution of the Ambiguities of Technology, or Why Bobby Can’t Spray“, Social Studies of Science 31 (4), p. 559.
[15] Ibid, p. 562.

reconstructed should be analysed in terms of **how a certain way of assessing the impact of a technology on security becomes dominant, including how security is being understood.** The following questionnaire can be used either for a number of interviews or for a workshop in order to produce the data needed to reconstruct the narratives:

Security Impact Assessment Questionnaire

The following questionnaire can be used either for a number of interviews or for a workshop in order to produce the data needed to reconstruct the narratives. The narratives to be reconstructed should be analysed in terms of *how a certain way of assessing the impact of a technology on security becomes dominant, including how security is being understood*.

1. Frequent and dangerous criminal actions

- What are the most frequent criminal actions?
- Why to they occur frequently?
- What are the most dangerous criminal actions?
- What makes these actions dangerous?

2. Security Measures and Technologies (SMTs)

- What kind of SMTs are being operated to deal with these criminal actions?
- Are there any major technological innovations that have been introduced?
- Are any technological innovations expected that will enhance the possibility to deal with them?

3. Impact of SMTs on criminal actions

- In which way have the SMTs contributed to security, and are there different dimensions of security affected?
- What is the impact of SMTs on crime?
- How is the impact being assessed / measured?
- When is an SMT ineffective?
- How do 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?
  - Unintended Consequences on freedoms?
  - Unintended Consequences on organizational routines (function creep)?
- To what extent have the promises of SMTs been delivered?

4. Preparation for database inclusion: Topics and Aspects

The following structure of topics and aspects has been developed in order to integrate results from work packages three and seven into the SIAM Online Assessment Support Tool. Questions will be added to the topics and aspects. The whole dataset to be integrated will then be documented in SIAM Deliverable 3.6. This data is a synthesis of the results of the empirical work and the literature analysis that has been conducted for work packages three and seven.

Topic	**Screen Heading**	**Aspect(s)**
Scope	Start the impact assessment on security with a description of the scope of the SMT.	Target Orientation (Groups, Area, Situations)
Topic	**Screen Heading**	**Aspect(s)**
Effectiveness in increasing security	Assess the effectiveness of the SMT in increasing security.	Indicators, Societal Dimensions, Efficiency, Calculability, Predictability, Control, Response Time
Topic	**Screen Heading**	**Aspect(s)**
Dimensions of Security	Understand different dimensions of security.	Shared understanding of security
Topic	**Screen Heading**	**Aspect(s)**
Establishing or maintaining a state of security	Assess aspects of establishing or maintaining a state of security	Prevention, Detection, Preemption, Security gain, Follow-up costs, Redundancy, Security Staff, Social Order, Expectations, Implicit Assumptions, Reliability,

		Unintended Consequences
Topic	**Screen Heading**	**Aspect(s)**
Mitigating or preventing threats	Assess aspects of mitigating or preventing threats	Security gain, False Positives, False negatives,
Topic	**Screen Heading**	**Aspect(s)**
Ensuring functional performance	Assess the functional performance of the SMT	Resilience against sabotage and / or cyber attacks, Reliability

Figure 1: Table of WP 3&7 Topics, Screen Headings and Aspects.