Criteria for Assessing and Mainstreaming Societal Impacts of EU Security Research Activities. Coordination and Support Action.

Good practice in SIA – Final Report

Deliverable 1.4

Technische Universität Berlin / King's College London

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 313062

Imprint

Responsible project partner:
Technische Universtität (TUB)

Author(s):
Lars Ostermeier, Barbara Prainsack

Contact:
Lars Ostermeier, ostermeier@ztg.tu-berlin.de

Barbara Prainsack, barbara.prainsack@kcl.ac.uk

ASSERT website

www.assert-project.eu

Version history

Version	Date	Change/Remark	Responsible (person, beneficiary/function)
1	23 April 2014	Added Section 5	Lars Ostermeier
2	25 April 2014	Revised report considering external reviews of D1.3	Barbara Prainsack
3	30 April 2014	Final Version	Lars Ostermeier /Barbara Prainsack

Acknowledgements: The ASSERT consortium is grateful to Dr Peter Mills and Professor Brian Rappert for very helpful comments on Deliverable 1.3, which have informed this Report.

TABLE OF CONTENTS

ANNEXES

1. Executive Summary

This Report presents the results of work package 1 in the ASSERT project. Its central part are nine 'good practice' principles for SIA developed by the ASSERT consortium. These principles are designed to guide those planning and carrying SIA in the security domain and beyond (2.1). The development of these principles has been informed also by insights and feedback obtained on the occasion of two workshops and one Masterclass organised by ASSERT in 2013 and 2014.

The Report starts by situating SIA within the Responsible Research and Innovation (RRI) framework. It argues that the goal of a wide acceptance and use of SIAs across different countries, fields, and contexts continues to be jeopardised by a lack of institutional embeddedness of SIA, as well as a fear of administrative burdens, both in terms of structures and working cultures. It then presents the nine good practice principles: Societal Security, Societal Impact, Reframing, Consultation, Flexibility, Iterative processes, Low Administrative burden, Limitations of SIA, and Knowledge. It argues that these principles, if implemented successfully, can also help to create more conducive institutional contexts and procedures for SIA.

The subsequent section (Section 3) focuses on the identification and discussion of 'intervention points' for SIA across different R&D phases: programme planning; project evaluation; project implementation; programme evaluation; and the use of research results. It discusses what forms SIA can take at different stages of project development, implementation, and evaluation.

Section 4 then introduces a concept for SIA training in the form of a Masterclass, and reports on the results of a first trial of the training exercise. It argues that the Masterclass is a promising concept for SIA training because it helps researchers, administrators, and policy makers to better understand conceptual and practical issues around SIAs. This ultimately contributes to an increase of the capabilities to plan and evaluate SIAs that are in line with the good practice principles. Following the first 'trial' run of the Masterclass, the ASSERT consortium has received valuable and constructive feedback from participants, which will be discussed in the final section of this Deliverable.

Section 5 discusses a number of important projects and documents featuring methods that reflect the state of the art of SIA in security research. This annotated collection highlights the contribution of these projects to ASSERT's objectives. It also responds to requests for a collection of these materials that have been voiced repeatedly in the context of ASSERT events and activities.

This Deliverable is an extended and revised version of an earlier report (D.1.3). The revision includes the comments form two external reviewers.

2. Good Practice Principles for SIA

The objective of this Report is twofold. First, it contextualises SIA in the emerging Responsible Research and Innovation (RRI) framework for security research (2.1) presents nine good practice principles that can be used to design SIA processes as well as to evaluate SIA plans (2.2). The second objective is to show how these principles can contribute to the effective use of SIA across all phases of the research and development process by different stakeholders. Drawing upon the results of two workshops organised by ASSERT, section 3 presents a typology of SIA in different phases of the R&D process. The fourth section presents the concept for a training exercise, the "ASSERT Masterclass", which was developed to enhance the capabilities of those organising and carrying out SIA to adapt the principles towards their needs. The final section summarises the results of a testing of the training concept.

2.1 SIA in the context of the Responsible Research and Development agenda

The development of good practice principles for SIA can help to mainstream and operationalise the objectives of the RRI agenda set out by the European Commission:

> [RRI] *refers to the comprehensive approach of proceeding in research and innovation in ways that allow all stakeholders that are involved in the process of research and innovation at an early stage (A) to obtain relevant knowledge on the consequences of the outcomes of their actions and on the range of options open to them and (B) to effectively evaluate both outcomes and options in terms of societal needs and moral values and (C) to use these considerations (under A and B) as functional requirements for design and development of new research, products and services. The RRI approach has to be a key part of the research and innovation process and should be established as a collective, inclusive and system-wide approach. (EC 2013: 3)*[1]

While we are sympathetic to the objectives of the RRI agenda, we remain cautious of overly instrumental approaches to achieve them. In addition, the definition's assumption that research and innovation take place in a linear manner – i.e. that research is carried out first and then 'translated' into applications – does not correspond with reality. In this sense, the RRI approach is in a tension with SIA as we promote it within ASSERT.

[1] It should be noted that this statement sets up RRI as a critical reflection on the social value of research, which is different from the original EU model that focused more strongly on extending regulatory oversight.

It is worth noting here that over the past three years, SIA has received explicit recognition by the European Commission's (EC). The EC's FP7 work programme for security research in particular stated that

> *Attention should also be given to the impact of the proposed technologies on the society, the organisational processes and the respect of legal requirements, such as respect for fundamental rights which must be embedded in each proposal and foreseen in the proposals' work plans.*[2]

The 2013 programme spelled out in more detail what attending to the impact of proposed projects should entail:

> *Proposals should consider possible side effects of technological solutions to security problems and assess alternatives with the least intrusive effects on privacy and freedom. A holistic approach to security will take the perception of citizens into account and focus on dimensions such as perceived security, while being aware of the fact that security risks can be unevenly distributed within and between societies. Proposers are encouraged to develop solutions strengthening societal resilience and active participation of citizens as security enhancing resources.*[3]

This objective became more formalised via the establishment of a 'Social Impact Check List' (developed by a working group) that any submitted proposal should consider (see Annex 5). In addition, the 2013 guide for applicants explicitly referred to the need to consider societal impact, and mentions that this will represent a criterion for evaluation:

> *Attention must be given to the societal impact of the proposed security solutions, which will be evaluated under the criterion "impact"*[4]

The good practice principles for SIA proposed in this report are destined to help SIA planners and implementers to avoid that SIA turn into merely tokenistic exercises, or that they become overly bureaucratic. This challenge is complicated by the fact that there is no SIA recipe that universally fits all projects. While some projects may require an extensive SIA with a dedicated project work package and an significant budget, other projects may suffice with demonstrating that they have considered possible societal impacts at the planning stage, and that they have the capacity to identify and address possible issues when they emerge. (This does not mean that the expertise to address issues and manage risks needs to be 'in house', but projects applicants should

---

[2] http://ec.europa.eu/research/participants/data/ref/fp7/89287/k-wp-201101_en.pdf [29 Apr 2014], p. 10.

[3] http://ec.europa.eu/research/participants/data/ref/fp7/192060/k-wp-201302_en.pdf [29 Apr 2014], p. 13.

[4] http://ec.europa.eu/research/participants/portal/doc/call/fp7/fp7-sec-2013-1/32752-fp7-sec-2013-1_cp_annexes_en.pdf [29 Apr 2014], p. 8.

typically be able to demonstrate that they know where and how to get help when needed). To what extent, in what form, and at what stage societal impacts are being considered in a given proposal or project needs to be decided on a case-by-case basis.

The good practice principles put forward in this Report are designed to accommodate also that research and technology development in real life are not entirely linear and rational processes but they also depend on serendipity and coincidence. It is thus important to retain a level of flexibility within good practice frameworks for SIA.

In the optimal case, SIA are a genuine learning exercise for all actors. So far, the acceptance and wider use of SIAs has been jeopardised by the lack of institutional embeddedness. The development of good practice principles also aims at improving this situation: SIA that are well conceived and carried out in a manner that is beneficial to all actors can help to create better support for SIA within research institutions, Higher Education Institutions and funding agencies.[5]

Before we turn to presenting the good practice principles, let us look at who should be in charge of planning and implementing SIA plans. A recent *Eurobarometer* study on RRI reports that more than three in four respondents agreed that the EU should take measures to address the ethical risk of new technologies.[6] Interestingly, public discourses about means to ensure that such risks will be addressed seem to be focused mostly on rights and ethics: "Most agree that respecting ethics and rights guarantees research and innovation will meet citizens' expectations" (Eurobarometer 2013: 112) While SIA is not mentioned explicitly in the *Eurobarometer* report as an approach to operationalise RRI objectives, it is noteworthy that the Report found a large preference for mandatory ethics trainings and even for an oath: "A large majority think there should be mandatory ethics training for researchers, and an oath taken to respect ethical principles and legislation" (ibid.). Two in three respondents said that scientists working at universities or in government laboratories should play a leading role in explaining the impact of science and technology on society. Scientists working for private companies were preferred by just over one in three respondents for this role (Eurobarometer 2013: 43). Only 4% said that politicians should play a major part here. A slim majority (55%) of all respondents considered public dialogue as necessary for decisions about science and technology being taken, while about one in three respondents said that such a dialogue was not required (Eurobarometer 2013: 41). Three in four respondents thought that the impact of science and technology on society was overall positive (Eurobaromater 2013: 51). In seeming contrast to the large support for mandatory measures, most respondents also expressed trust in scientists: "At least eight out of ten think that scientists working in government laboratories or universities (82%) and environmental protection associations (81%) try to behave responsibly towards society by paying attention to the impact of their science and technology related activities" (Eurobarometer 2013: 56).

This short glance at the recent *Eurobarometer* survey highlights the relevance of SIA for R&D. It appears that SIA needs to be brought from the policy making level into the

[5] This objective has been formulated in one of the recent Horizon 2020 calls: Topic ISSI.5.2014.2015 - Supporting structural change in research organisations to promote responsible Research and Innovation in the H2020 Workprogramme „Science with and for society", p.25.
[6] http://ec.europa.eu/public_opinion/index_en.htm

project implementation level in order to give academics and scientists more prominence in the planning and implementation of SIA, while at the same time refraining from increasing the bureaucratic burden on researchers and administrators. At the same time, the *Eurobarometer* survey shows that a conflation of societal impact with 'ethical' challenges seems to prevail. This narrow understanding should be overcome.

2.2 SIA Good Practice Principles

In a previous report on methodologies relevant to the assessment of societal impacts of security research in work package 1 of the ASSERT project (Prainsack/Ostermeier 2013), we concluded that "[a] core challenge of SIA at present, according to Vanclay and Esteves (2011: 4), is to find ways to communicate more effectively, and to demonstrate the value of SIA more clearly." Drawing on evidence from our research in ASSERT, this observation still holds. ASSERT have organised two workshops and one Masterclass in the recent six months. At these events, participants discussed the results of our research and provided useful input into our ongoing work. It appears that in the domain of security research, levels of awareness and acceptance of SIA have so far been relatively low. Especially traditional industry and security actors seem to see SIA as an obstacle rather than a benefit for research and technology development. Among policy planners, evaluators and research programme implementers, there appears to be little awareness of how SIA could benefit their work and how SIA should be implemented. Even researchers sympathetic to the ideas associated with SIA are unsure about how to include such assessments into their activities at a practical level. This Deliverable therefore sets out to develop good practice principles that are based on lessons learnt from a review of the literature, from the discussions at ASSERT events, and on the comments of our external reviewers (see above, Acknowledgements).

Our good practice principles draw upon relevant literature within the areas of SIA, constructive technology assessments (CTA), and privacy and surveillance impact assessments (PIA/SuIA). We fully endorse Arie Rip and Johan Schot's understanding that fruitful research and technology assessments are "not about predicting possible future impacts of the technology as accurately as possible – rather, [their core value] lies in the dialogue and the interaction it requires the actors to engage in, while developing a technological solution" (cf. Kreissl et al. 2014: 4). Interestingly, speaking from an industry perspective, Harvey (2011) reached a similar conclusion, voicing the need for better training of experts in charge of planning SIA processes, so that they conceive these assessments not merely as a tick-box exercises or as the development of return on investment plans, but as ongoing processes that facilitate a deeper understanding of the core societal issues at stake and genuine dialogue among the stake-holders. Harvey (ibid.) describes three main 'schools' of SIA as follows:

1. **Pragmatic school:** SIA configured to the compliance required of host jurisdictions'

2. **Procedural SIA**: focus on in-depth understanding of the core issues, and often on creation of consensus among stake holders

3. **Return on investment for societies**: Quest for increasing social benefits of planned interventions

Box 1: Harvey's three SIA 'schools' (adapted from Harvey 2011)

It is clear that a tokenistic exercise in terms of Harvey's first school (see Box 1) would be of little help to anybody except those getting paid to carry out SIA. Although a return-on-investment approach could be desirable in the views of some stakeholders, the scope of this approach is not in line with good practice principles developed in this Report. The second school seems the one to meet the generic criteria outlined above the best. *The character of the second school renders SIA an iterative process that allows intervention at different points in time, with different methods that share in common the normative assumption that a dialogue of stakeholders itself is a benefit*. This also suggests that training researchers and practitioners to carry out SIA may be a better strategy than prescribing certain ways to organise them. In other words, rather than educating potential planners and implementers of SIA procedures to follow pre-determined recipes, it is important to put them in a position to plan SIA procedures that meet good practice criteria and accommodate the specificities of their specific projects and contexts at the same time.

Knowledge, Power and conceptual issues of SIA

The importance of SIA training becomes even more evident considering the trend in the SIA literature from context-neutrality towards contextualisation.[7] This trend can be understood as a reaction on the frequently cited 'obsession' within much of the SIA literature with methods and procedures rather than the focus being on the outcome and the impact of a certain project. SIAs should thus never turn into mere risk assessment exercises. While it is certainly important to identify risks and to take appropriate measures to pre-empt, minimise, or mitigate them, it is equally important to understand SIA as a process that broadens the range of alternatives by *reframing* an issue instead of sticking to "a pre-determined range of possible alternatives" (Prainsack/Ostermeier 2013: 17).[8] Such reframing can entail a redefinition of what should be considered a 'risk', or how risks should be assessed and classified. The potential of the SIA design to reframe the project and R&D process is therefore crucial. Such reframing needs to be at least informed by – if not take place in collaboration with – relevant stakeholders and communities. A starting point for this collaboration is the explication of a shared understanding of societal security. Related to this, it is important to spell out how the societal impact of a research programme, a project, or a product, is conceived.

While the concept of societal security lacks a coherent definition, its benefit for SIA is that it foregrounds the procedural dimensions of security (Buzan et al. 1998). Authors working in a project on *European Security Trends and Threats in Society* (ETTIS) have defined societal security as "*the security of societal sources of human well-being* in general, and *the societal sources of individual security* in particular" (ETTIS 2012: 23,

[7] With contextualisation, we refer to the acknowledgement of the need to adapt generic principles for SIA to specific contexts where those principles are being applied (see for example Vanclay 2003).
8 The collection and analysis of cases where SIA procedures successfully reframed the goals/methods is an important task for future research.

original emphasis). The concept signifies "ultimately what different societal actors perceive as societal security. By its very nature, societal security is continuously in the making, and it harnesses a variety of stakeholder perspectives" (ETTIS 2012: 4). In general, according to the ETTIS consortium, the concept of societal security is concerned with four aspects: definitions, dimensions, sources, and societal security strategies & governance (ibid.).

SIA Good Practice Principle 1:

Clarify how societal security is understood in a given project (especially when this is implicit).

An explicit reflection on how a project is likely to impact on societal security requires SIA planners to reflect the implicit understanding of security and how their project is related to this understanding. Reflecting on the concept societal security to be employed in a particular SIA is also helpful to overcome what has been called 'technology fetishism' in security research. 'Technology fetishism' refers to the suggestion of ever more technological 'fixes' for inherently societal issues (see Hayes 2009 and IRISS 2012). Considering the four aspects of societal security identified in the ETTIS Report (see above) in connection with the planning of SIA, it becomes clear that SIA planners need to consider and make explicit how societal security is defined and delineated, and what factors are likely to impact on societal security (ETTIS 2012: 7).

SIA Good Practice Principle 2:

Clarify how societal impact can be operationalised in the context of a particular project.

What questions do you need to ask in order to find out what, how, and when factors will likely impact society? In Deliverable 1.2 we emphasised the need to render SIA an assessment of *societal* impacts, including a much broader scope of SIAs than approaches referring to *social* impact assessments (understanding them as those impacts that have not yet been assessed in ethics or legal compliance reviews). SIA planners and implementers should thus use an inclusive definition of impacts as comprising benefits, unintended consequences, harm, etc. Furthermore, societal impacts can include impacts on individuals, households and enterprises and communities at each level of society. It is important to avoid limiting the scope of an SIA plan to those directly and obviously affected by a project but to include also those who may be affected indirectly. Wadhwa et al. (2014) provide practical step-by-step guidance on how to identify societal impacts, and Annex 3 includes a list of questions geared towards understanding issues pertaining to public accountability and the distribution of power in a project in particular.

SIA Good Practice Principle 3:

Give the SIA design the potential to reframe the project and R&D process.

The extent to which there is potential to reframe the goals, categories, and methods of the project will largely depend on how open the outcome of the process is. If very specific deliverables have been promised, then the capacity to change or modify the project are more limited than if the deliverable specification was more open, allowing for the inclusion of unanticipated findings and results. This also raises the question of whether or not there should be criteria that, if met, would lead to the abandonment of the project altogether. While the latter is not a possibility at present in most R&D projects in the security research domain, it is important to carry out a threshold analysis at the pre-application stage to determine whether or not the inclusion of the scenario of project abandonment is necessary. Pertaining to a less 'extreme' scenario is the question of whether and how the core mission or stakes of a project can be modified while it is under way. This question needs to be addressed both in terms of its implications for research activities as well as in terms of project management and reporting.

SIA Good Practice Principle 4:

Take participation seriously. 'Participation' of relevant people and groups means more than merely to inform or consult them.

Closely related to the modification of goals, categories, and methods is the topic of public, user, and stakeholder participation. While participative approaches in research are becoming increasingly common in both applied and basic research, reviewing the relevant literature (see Prainsack/Ostermeier 2013) one frequently encounters the concern that too often, participation is being considered not as an opportunity for genuine learning but an 'education exercise' to create consent and acceptance among those who may be skeptical. In other words, participation serves the purpose of reducing friction points and increasing acceptance (see also Bogner 2012). In order to avoid such an understanding of participation and to facilitate opportunities for genuine learning, it is important to render power differentials visible and put them on the discussion and negotiation agenda (see also Wadhwa et al. 2014). Questions to be discussed include: Who is likely to benefit from the research that the project sets out to do? How are they likely to benefit, and at the cost of whom? Who will be empowered and disempowered by this research (see Prainsack/Toom 2010)? Who is likely to suffer adversity, and how can these asymmetries be balanced? What are the external factors of the project impacting on the research activities?

Attempts to plan and manage the societal impact of security research projects will need to produce knowledge about how users, stakeholders, and publics can be included in the most fruitful manner. One way to facilitate the careful consideration of issues pertaining to the nature and format of participation is to explore the distribution of power and agency following the guidance by Prainsack (2014, see for details Annex 3). In cases where such a deeper assessment cannot be carried out, it is important for SIA plans to at least make explicit who is in the position to define what is important and

less important. Furthermore, the roles and responsibilities of all project participants (and users and other stakeholders that are included in the project) need to be clearly defined from the beginning on. Any kind of user, stakeholder, or public participation should be conceptualised as a process that is supposed to have an impact on security research and not to create acceptance or reducing opposition. It is in this line of thinking that "a dialogue among different individuals and groups who are considered (or consider themselves) as potentially affected by a planned project is a benefit in itself" (Prainsack/Ostermeier 2013: 5). It needs to be emphasised, however, that it is important for SIA planners and managers to act upon the constructive "irritation" that this dialogue can create (e.g. by adjusting or amending the project's goals, methodologies, user engagements, etc.).

The conceptualisation of SIA as a genuine learning process as opposed to a risk management process constitutes a major difference that allows for the identification of a number of more specific best practice principles, reflecting reservations against an overly instrumental take on SIA. One of them is *flexibility* that should allow to sufficiently accommodate the impact of a SIA process.

SIA Good Practice Principle 5:

Make sure that the SIA process is flexible.

Project managers and researchers will need to determine the level of flexibility within a SIA that ensures that it can adapt and adjust to new evidence, new insights, or changes in the project. Closely related to the need for flexibility is the need to design SIA in such a way that it can be implemented from the earliest stages of the project. Equally important is to ensure that results of SIA are fed into the R&D process.

SIA Good Practice Principle 6:

Create feedback loops between SIA and the rest of the project / programme.

Deliverable D1.2 of the ASSERT project concluded that "In this spirit, the main outcome of ASSERT should be a resource that requires and structures critical reflection, guiding and facilitating the conduct of societal impact assessment…" (Prainsack/Ostermeier 2013: 5). This objective entails that SIA are embedded in a process where the overall R&D on the one hand, and SIA on the other, are carried out in an iterative manner. This poses the risk a second layer of project planning and management emerges. This can a burden for research budgets and another strain on the limited time that researchers have available and should thus be avoided. What every SIA can do, however, is to facilitate iterative processes wherever this is meaningfully possible (e.g. where project participants support this and see this as a benefit).

SIA Good Practice Principle 7:

Keep the administrative burden reasonable.

While the criteria for what is 'reasonable' clearly depend on the specifics of a project, in general, one way to ensure that the administrative burden posed by SIA is kept at a reasonable level is to redesign existing assessment processes that are already in place. For example, the scope of ethical review procedures – where these are in place – can be expanded to include SIA. In some cases, SIA can help to actually decrease the overall administrative work within a project. This can be the case when SIA help to detect possible problems early and thus avoid the loss of time and money later on.

It is also important to be very explicit vis-à-vis those who may be skeptical about the value of SIA about why, at certain stages in the process, SIA might create extra work, and how this benefits the overall project. If the possibility of additional costs – in the widest sense of the word – and the likely benefits are not spelled out from the start, support for SIA is likely to suffer.

The research carried out within ASSERT also highlights the importance of understanding the difference between SIA on the one hand, and evaluation on the other, when planning or managing SIA processes. Although the two processes can overlap, their points of gravity are different: While SIA typically are prospective, evaluations are typically retrospective. It is therefore important to define what the focus of the prospective scope should be: unintended consequences, questions regarding who benefits, or positive outcomes? This process includes far-reaching decisions about what needs to be known, what can be left aside, and possibly even what should be concealed in SIA processes. Furthermore, it should be made clear in the SIA plan who has access to which kind of knowledge, and to highlight to what extent transparency is desirable: are there situations where transparency cannot or should not be achieved? Rappert (2012), for example, has shown how ignorance and concealment contribute to the production of order in negotiation and assessment procedures in the international security policy-making domain. This approach, and the literature on "ontopolitics" (Mol 2003), can make a fruitful contribution to the conceptualization of transparency in SIA processes by showing that transparency and accountability always involve decisions about issues that should *not* be made transparent.

SIA Good Practice Criterion 8:

Think about transparency and the limitations of the SIA process.

In terms of the temporal scope of SIA procedures, one reason why it is important to consider the timescale of SIA from the start is that in some cases, it is useful for SIA to continue for a while after the rest of project has come to an end. This could be particularly fruitful in projects where the societal impacts are expected to be considerable and/or to manifest themselves mainly after the end of the project. This may pose practical challenges, however, budget constraints may render it unlikely that serious attempts to manage the impact of the results will be made. If these obstacles cannot be overcome, then these limitations should be acknowledged explicitly from the

start: Awareness and transparency about such limitations increases both the *transparency* of the SIA procedures as well as an understanding of its *limitations*. Furthermore, a clear statement about the societal impacts that have not been taken into account in the SIA management plan can help to avoid misunderstandings about the remit and scope of a particular SIA process. A relevant example for in terms of the geographical scope is the proliferation of security technologies in countries outside of the European Union. NGOs like *Statewatch* have repeatedly voiced concerns that efforts to strengthen the consideration of ethical and societal issues in security research are of little value if findings and products are developed for export to markets outside of the European Union.[9] The transnational dimension of impacts tends to be neglected in the SIA literature.

Besides the inevitable limitation that access to relevant data and information tend to be restricted in many contexts in the security domain, other likely limitations pertain to resources (budget and personnel). Moreover, related to user involvement, stakeholders, and publics, even the most participatory approaches will have limitations, which should be openly talked about (also with users, stakeholders, or members of the public, before they agree to participate. The latter point is relevant also regarding the objectives of the dissemination strategy, which should aim at communicating the results of the project and the SIA process, but not to simply 'sell' it. In all ASSERT workshops, considerable emphasis has been placed on the use of social media as a means to communicate with the broader public beyond the SIA processes.

Practice Criterion 9:

Clarify what purpose the knowledge in a SIA should serve.

Do you want to use it primarily within the project itself, to make the project more socially robust? Do you want to use it to communicate with policy makers? Do you need it for an evaluation report? Our consultations with experts and stakeholders have consistently shown that there is a need to specify what kind of knowledge is being produced in a SIA. It may be helpful to differentiate between scientific knowledge, knowledge for political and societal decision- making, and risk management knowledge. While these categories clearly overlap in practice, explicating what purpose knowledge-production is destined to serve will help to ensure that the knowledge produced in the SIA is *relevant* for this purpose (or these purposes). Being conscious of the type of knowledge that SIA are expected to produce also helps to avoid that the outcome of SIA are prejudiced by using inadequate causal assumptions and definitions (Cashmore 2004: 422). Precisely for this reason SIA cannot and should not be expected to meet academic standards in knowledge production and analysis.

In terms of the kind of data produced and analysed, projects such as the VALUESEC project have shown that impact assessments will virtually always need to include qualitative data, if not solely, then in addition to quantitative data.[10]

[9] See for an example on spying software proliferation: https://citizenlab.org/2013/03/you-only-click-twice-finfishers-global-proliferation-2/ [26 Apr 2014]
[10] http://www.valuesec.eu/content/valuesec-project [26 Apr 2014]

3. SIA across the different phase of the R&D process - a phase approach to SIA in security research

We have argued in the previous chapter that good practices in SIA need to consider political dimensions of knowledge and power as well as some conceptual issues. Planning and doing SIA always means to stimulate, initiate and potentially moderate broader societal debates. Therefore, we have suggested that SIA approaches should not be mere consultation exercises enhancing the effectiveness of security research in terms of facilitating the implementation and acceptance of security policies. The development of more specific good practice criteria, as well as guidance for the implementation of these criteria, requires a specification of the contexts in which SIA are used. Very similar to the phases of the R&D process that have been defined by the ASSERT consortium (see below), a report by the Societal Impact Expert Working Group has listed five phases of security R&D:

1. Work Programme & Annual calls;
2. Proposals;
3. Negotiation;
4. Project Execution;
5. Implementation of a completed product, system or techniques in different contexts (CIES 2012, p. 11).

When planning and managing a SIA process, it is important to consider in what phase they should be implemented. In each of these phases, the goal orientation, openness, stakeholders, methods/procedures and the outcome of the SIA will be different.

At a workshop in November 2013 in Berlin, the ASSERT project invited 30 experts from the security research domain to discuss questions pertaining to the implantation of SIA in different project phases. The objective of the workshop was to identify end user needs, requirements and best practices in social impact assessment (SIA) in security research and to discuss the transferability of approaches from other research domains.[11] The range of experts participating this workshop included those working in programme planning at national levels and at the European level, evaluators of FP7 projects, research funding administrators, those implementing research projects, and experts delivering products for end-users. This chapter is informed by the views and positions expressed by workshop participants.

The workshop was structured in two main parts. The first part, *setting the agenda*, determined the state of affairs in social impact assessment in security research with a breakout/brainstorming session: what are current trends in SIA, what kind of approaches have been tried out, what are the lessons learnt from early attempts to implement SIA in security research? In the second phase, *taking SIA in security research to a new level*, we presented an overview of innovative and deliberative good practices / methodologies for social impact assessment both in security research and other research domains that has been developed drawing on literature reviews and a

[11] These were discussed at the first workshop in in September 2013 at King's College London.

workshop on transferability of SIA approaches from other research domains (Deliverable 1.2). In the final session, we asked experts to identify key requirements for the fine-tuning of the ASSERT methodologies, with a focus on the research phase, best practices and lessons learnt.

The results of the workshop contributed to:

- The identification and specification of end user needs and requirements for the development of a security impact assessment tool.
- An overview of best practices of SIA for different phases: research programme planning, evaluating proposals, funding and implementing research programmes, and implementing research projects.
- An overview of 'drivers' and 'spoilers' for transferring SIA approaches into the security research domain.
- The formulation of recommendations for further enhancing impact assessment approaches.

3.1 ASSERT TUB workshop Day 1

Sessions on existing approaches of SIA, current trends, and lessons learnt

At the beginning of the workshop, the invited experts presented their perspectives and experiences on existing approaches in SIA, current trends, and lessons learnt from their own work and practice.

A representative of the Austrian Ministry of Transport, Innovation and Technology talked about the KIRAS Security Research programme (kiras.at/kontakt/). KIRAS consists of three main pillars: economic aspects, security policy, and socio-economic aspects. The understanding of security underpinning the programme is an inclusive one. It aims at facilitating solutions that improve both liberty and privacy, and that at the same time link Austrian security research into European programmes for research and innovation. It also employs an integrative research approach that does not treat technology as the answer to everything. As was specified, such an approach is feasible in Austria, because the country lacks the famous military-industrial complex, and is characterised by the absence of large commercial enterprises in the security domain. Most commercial actors in the security domain in Austria are small and medium-size enterprises (SME). It is a requirement of the programme call that all projects include HSC (humanities, social sciences and cultural studies) and end users. These are eligibility criteria. Specifically, KIRAS has five main goals: to improve measures of objective and subjective security; to generate knowledge necessary for the achievement of Austrian security policy goals; to facilitate the development of security relevant ethnology leaps; to aid the growth of the security industry; and to help to achieve excellence in the area of security research. The national steering committee consists of all ministries and stakeholders relevant for security research. The Ministry of Transport, Innovation and Technology is the programme owner and funding authority of KIRAS.

A REA representative then outlined the role of societal impact assessments within the new Horizon 2020 (hereinafter: H2020) programme. Questions about societal impact will be part of standard proposals (in the form of a narrative self-assessment and yes/no questions, plus reference to relevant pages in the proposal). In the Q&A session that followed, questions about the unintended consequences of this development were raised: could it be that security companies will stop wanting to come on board as project partners because they are afraid that the inclusion of SIA (and the social science aspects included in the project) may slow them down? A good response to this concern, perhaps, is a reference to the experience of grant programmes in the UK and at the European level, where initially, the inclusion of ethics and social science aspects was considered a nuisance by many life science and industry partners. Today, many of them see the added value that the inclusion of these aspects brings to a project.

A senior researcher from the University of Bergen presented EPINET (www.epinet.no), an FP7-funded project exploring the impacts of science and technology on society and the environment from different disciplinary, conceptual, and practical perspectives. Instead of assessing the impact of these technologies at a hypothetical level or in the abstract, the project carries out assessments of 'technologies in practice'. The assessments include, from the very beginning, the users envisaged by the project, as well as policy makers and technological innovators. A result is that 'as soon as you start to engage with these people, things are getting messy - you don't know who is doing what, and everybody is doing a bit of everything'. At the same time, there are clear benefits of bringing together actors that normally do not speak to each other. These benefits include the increase of participants' awareness of different positions and perspectives, the broadening of the scope of the impact assessment (to ensure that nothing important is left out), and the creation of new stakeholder networks. In some cases, dialogue between opposing parties can also resolve differences and in that way benefit the project by avoiding cost and conflict further down the line.

A representative of the Technology Foundation, Berlin, argued that one of the challenges in the security domain is that the pool of end users includes potentially everybody. In contrast to technology development in the medical domain, where a knee joint replacement, for example, has a relatively clearly delineated group of potential users, the users of technologies used for airport security is the general population. The meaningful engagement of end users thus becomes an issue: who do you engage, and how do you ensure that they do not drop out? Technology developers in particular are at high risk of leaving the SIA process; they may be afraid of bad press as a result of attention being drawn to problematic aspects of a project. Moreover, SIAs are seen to have tangible consequences such as slowing down the innovation process, putting people on a list of 'suspects'. The introduction of biometric controls at Frankfurt Airport, for example, was completed after years of testing and adapting the technologies and processes. Moreover, 'perceived' impacts are not clearly separable from 'real' impacts; a merely 'perceived' impact can have 'real' consequences. In the ensuing discussion Uwe Weigmann referred to a participative assessment project called *Technology Workshops* that he organised for the new airport in Berlin.[12] He said that

[12] The airport's website is currently available in German only: http://ber.berlin-airport.de (accessed 2 March 2014).

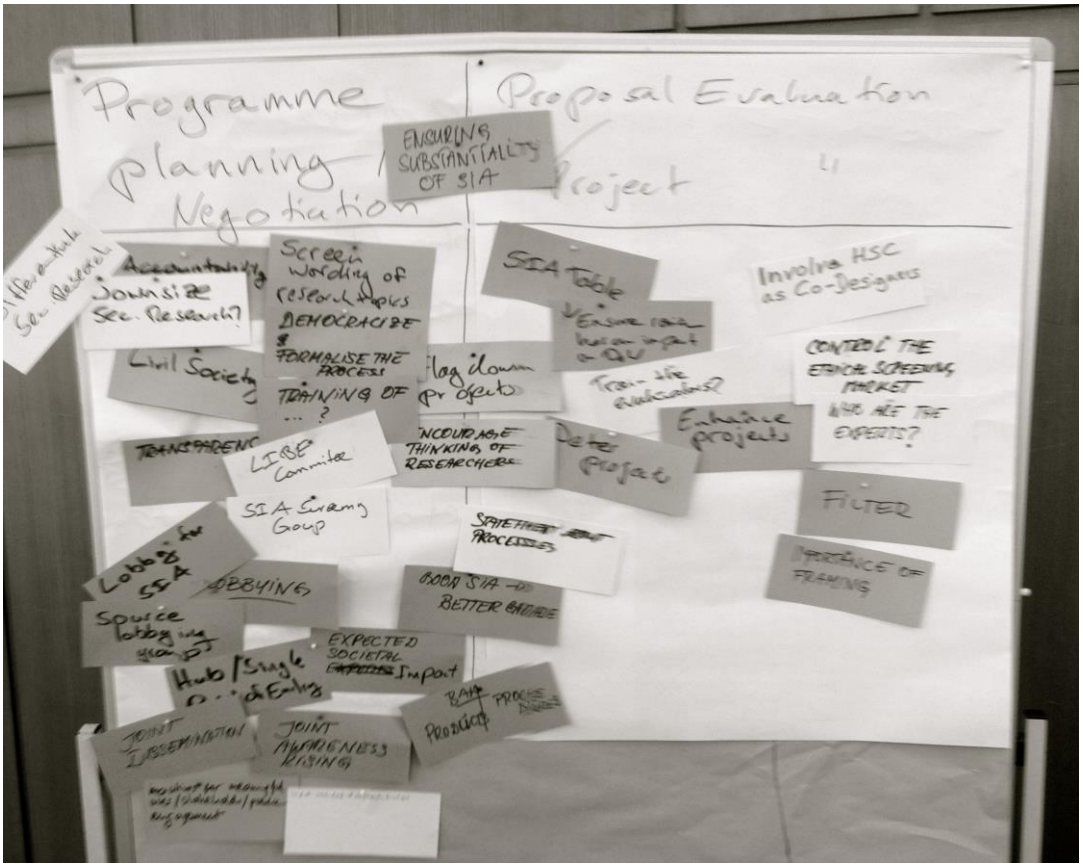
the process, including closed and public sessions, led to a better-informed decision making process and to a better acceptance of new technologies by employees.

The final session of the day started with a presentation on *Transfer of Best Practices and New Approaches for SIA in Security Research* by the authors of this report. Resonating with the issues raised by Uwe Weigmann, the discussion focused on security being inherent in almost every sector in public policy. Finding the right people to talk to can thus be a difficult challenge. Also hard-core 'techies' can be convinced of the value of SIA if they are told that SIA can increase acceptance (however the term 'acceptance by design' was criticised heavily).

3.2 ASSERT TUB workshop Day 2

Session on Challenges and new approaches for SIA in security research

The programme for the second day included a major brainstorming session on challenges and new approaches for SIA in security research. The authors of this report first presented a typology of SIA in different phases of the R&D process (structured along different phases and possible 'intervention points'). The participants were then asked to make suggestions and to discuss what could be done to do or to enable or improve SIAs in the different phases. The participants put their suggestions on cards and pinned them to the phases where the suggestions apply, creating a table of suggestions for SIA across the whole R&D process.



Picture 1: Workshop results for R&D phase 1 & 2 [photo taken by authors]

3.2.1 Programme Planning

The programme planning phase of the R&D process includes the entire decision making process, from the beginning of talks and negotiations about the content of a particular call up to the publication of new research programmes. This includes also consultations in connection with, and evaluations of earlier programmes. Participants at our workshop argued that civil society should be better represented in this phase in order to give societal perspectives more weight. Furthermore, most participants were strongly in favour of increasing the public accountability of the decision making process pertaining to the content and focus of research and innovation programmes nationally and supranationally. Several experts reported that the often decisive influence that political considerations had on funding programmes, often exercised at the final preparation stages leading up to the publication of the call, frustrates attempts to increase participation and accountability in the programme planning phase. A more clearly and transparently structured process of programme planning, it was felt, would increase the democratic character of civil security research (and research more generally). Increasing transparency and introducing a more structured approach were also seen as necessary against the backdrop of growing overlaps between military/ and civil security industries. One participant argued that the military-industrial complex has been replaced by the security-industrial complex, raising crucial issues of dual use.

It was suggested also that discussions about societal *needs*, instead of societal *impact*, could help to address problems resulting from unduly narrow and formulaic definitions of security. Formulaic definitions typically endorse an 'elite approach' to defining security, in the sense that security agencies define threats, and there is hardly any chance to validate them because the knowledge needed for validation is not accessible to anybody outside of the security agency domain. This, in turn, leads to a tendency to define security as a set of threats that can be countered with technologies in the programme planning phase. This narrow definition as security as a set of threats in need of a technological fix then determines the questions that are being asked during the planning phase: it is more about technologies than about societies who are supposed to benefit from those technologies.[13] The concept of societal security can facilitate the introduction of a broader and more inclusive understanding of security into the programme planning phase.

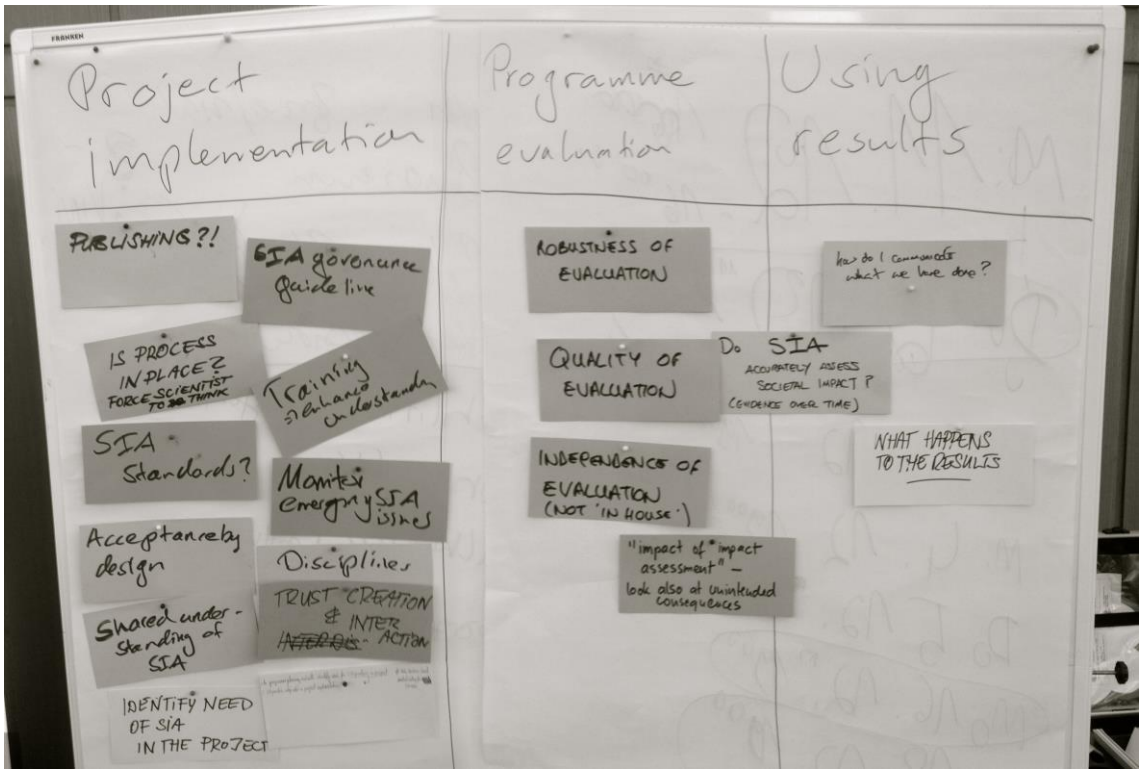
On a more practical level, the greatest opportunity to change the character and content of research programmes lies in the programme planning phase. In order to seize this opportunity, participants suggested to include a SIA screening or threshold analysis procedure in the phase of programme planning to identify topics and calls that are considered critical in terms of their societal impact at an early stage. A decision would then be made to either stop activities in a research area, or to highlight the research areas for their societal impact sensitivity. Such 'flagged' programmes or topics could then undergo a deeper SIA as a mandatory step of the procedure, and/or they could be required to define criteria that lead to the abortion of projects if met. In terms of transparency, some participants suggested to increase lobbying activities that aim at increasing public awareness of the societal impact of security research. This would contribute to both increasing the pressure for a more thorough consideration of societal impacts and to increase the understanding for the incentives that can result from SIAs for research programmes.

3.2.2 Project Evaluation

The evaluation of projects is a highly bureaucratic phase of the R&D process, and the vast majority of participants felt uncomfortable with suggestions to increase the administrative burden in this phase. Suggestions to increase the relevance of SIA in this phase, it was felt, should primarily aim at amending and increasing the efficiency of existing procedures. For example, very little information about the impact of the ethics screening procedures on research projects is available to the public. An evaluation of the nature of changes to project design and project implementation resulting from ethics screenings would provide for a better understanding of the merits and flaws of the existing ethics procedure. And more transparency during the ethics screening would facilitate the development of best practices. Some participants also suggested SIA training for ethics evaluators, as societal impact is a much wider remit than ethics.

[13] The Nuffield Council on Bioethics (NCoB) report on Emerging Biotechnologies reports the prevalence of the same idea, namely that social problems are 'fixed' with technological solutions, in the area of biotechnologies (NCoB 2012).

Accountability was another issue raised by the participants when the SIA table for FP7 proposal templates (see Annex 5) was discussed. While the overall structure of the table, and especially the combination of tick-boxes with qualitative information, has found a favourable reception, the impact of the table on the evaluation process is unclear to most participants. Especially methods that combine tick boxes with narrative answers were be considered very helpful, because they disclose a lot about how people go about thinking about ethics. It appears that while the table *can* have an impact on evaluations, this is not always the case. This leaves both proposers and evaluators in a limbo, possibly reducing the positive effects that the table could have on proposals and evaluations. It was therefore suggested by the participants that the SIA table should be made an integral part of the project proposal evaluation, whereby proposers should be asked to comment briefly on each phase and aspect. Participants in this discussion also mentioned that at the proposal evaluation stage, efforts should not only focus on whether societal impacts have been 'described', but on whether there is any evidence that project proposers have a sense of an ongoing exploration of societal impacts throughout the project.



Picture 2: Workshop results for R&D phase 3 to 5 [photo taken by authors]

3.2.3 Project Implementation

Together with the programme planning phase, the project implementation phase was seen by participants as a crucial phase where SIA could play an important role. This has implications for who should be doing SIAs. In the programme planning phase, policy makers, scientists and academics as well as civil society representatives need to be included into SIA processes. However, it is likely that policy makers will take the lead here. In the project implementation phase, in contrast, it is scientists and academics

who are responsible for developing and implementing SIA plans. Participants felt that the project planning and implementation phases are not distinct but they are connected, and that thinking about implementation should start with proposal writing. The role of science administrators in carrying out SIAs was considered of limited relevance here because the initial plan for SIA needs to be provided by those who will carry out the actual research.

One issue that the ASSERT consortium took very seriously was the demand for SIA training for scientists. Intense discussions took place about the German and Austrian national approaches to mandatorily include experts from the humanities and social sciences (HSC) in security research projects. Some participants said that they observed a change in the overall culture of planning and carrying out security research projects as a result of the mandatory inclusion of HSCs, towards a greater acknowledgement of the societal dimensions of security research to the benefit of all partners. That the exact role of HSCs in the process, however, inevitably needs to be determined from case to case enables consortia to (mis-)use them as merely a 'fig leaf'. In the spirit of the good practice principles it will be impossible for SIA planners in most cases to deliver a pre-determined outcome for SIA planning, but it will be possible to train SIA planners and implementers in the relevance of good practice principles. During the workshop, it was suggested that any SIA plan should include the following:

- SIA governance guidelines;
- a plan for the analysis and monitoring of emerging SIA issues;
- a statement about shared understanding of (societal) security and the societal impact;
- mechanisms to facilitate trust-building;
- plans for the publication of the outcome of the SIA process;
- plans for regular interactions between SIA stakeholders.

Participants at the workshop were in disagreement about whether or not acceptance for a project and/or technology through a SIA plan could be increased, and whether this should even be seen as a goal to strive for. Some argued that this could be a major incentive for some actors involved in the research project, while others said that this would undermine the overall purpose of SIA processes.

3.2.4 Programme Evaluation

With regard to the evaluation phase, participants highlighted the importance of ensuring that the results of the evaluation have consequences. Some participants felt frustrated by what they perceive as a lack of political will to act on the results of security research programme evaluations in particular. This was combined with the perception of a tendency to frame critical issues as a matter of programme administration rather than planning. Other participants felt that project evaluations would improve if more independent evaluators participated. The latter would also enable a stronger focus of evaluations on unintended consequences, which to date are almost completely ignored.

3.2.5 Exploiting research results

The extension of SIA plans to the phase of disseminating and exploiting project results was described as a very pressing issue. It was suggested that a separate section should be introduced to into the SIA plan dedicated to the use of projects results after the end of the project. In that section, project participants (and/or those in charge of SIA within the project) should be asked to specify actions and measures that aim to ensure that the project results cannot be used in ways that undermine the envisioned societal impacts or create unintended societal impacts.

The following table presents an overview of good practice principles, mapping against each phase according to the workshop results.

Good practice criterion	Programme planning	Evaluation	Programme Implementation	Project Implementation	Exploiting research results
Change	High possibility for change	Change following pre-determined criteria	Small possibility for change	Change following pre-determined criteria	High risk for unintended use of results
Participation	Good possibility for very broad participation	Small possibility for broad participation	Small possibility for broad participation	Good possibility for relatively broad participation	Difficult to determine
Flexibility	Very high flexibility	High flexibility in terms of deterring or enhancing projects	Flexibility according to criteria set in the planning phase	Flexibility according to the SIA plan	Very high flexibility
Iteration	Iteration in terms of learning from past experiences needed	Iteration in terms of possible recurring evaluations of SIA critical projects	Iteration mainly in terms of organisational learning	Iteration very important throughout the project	Difficult to determine
Administrative Burden	Highest possibility to increase administrative burden for democratic decision making	Very small possibility for an increase of the administrative burden	Very small possibility for an increase of the administrative burden	Very small possibility for an increase of the administrative burden	n/a
Transparency	Very good possibility for high transparency	Limited chances for full transparency due to privacy concerns	Limited chances for full transparency due to privacy concerns	Very good possibility for high transparency	Probably high administrative burden for transparency in this phase, needs monitoring

Limitations / Scope	Very high need for a clear statement of the scope of the SIA process.	Very high need for a clear statement of the scope of the SIA process.	Very high need for a clear statement of the scope of the SIA process.	Very high need for a clear statement of the scope of the SIA process.	Very high need for a clear statement of the scope of the SIA process.
Societal Security	Very high need for a clear definition of societal security	Very high need for a clear definition of societal security	Very high need for a clear definition of societal security	Very high need for a clear definition of societal security	Very high need for a clear definition of societal security
Societal Impact	Very high need for a clear definition of the societal impact	Very high need for a clear definition of the societal impact	Very high need for a clear definition of the societal impact	Very high need for a clear definition of the societal impact	Very high need for a clear definition of the societal impact
Knowledge Type	Knowledge for decision making	Knowledge for decision making	Knowledge for management and administration	Knowledge for project management and planning of research activities	n/a

Table 1: Overview of good practice principles, mapping against each phase according to the workshop results (this table will be revised further following the results of discussions at the 2nd ASSERT Masterclass on 29 April 2014).

4. The ASSERT Masterclass

4.1 The Masterclass concept

The ASSERT Masterclass was developed and launched by the members of the ASSERT consortium. The motivation behind the Masterclass was to provide a structured learning environment for scientists, academics, administrators, evaluators and policy makers that increases their capacity to plan and to manage SIA in the security research domain. The Masterclass was first 'trialled' on 20 invited participants in early February 2014 in Stirling, Scotland.

The Masterclass was structured in two main parts. In the first part, background information about SIA concepts and methodologies – many of which were addressed in Deliverable 1.2 – were presented and discussed. The objective of the first session was to help participants to develop a good understanding of the concept of societal impact assessment (SIA), of the core underlying concepts and theoretical approaches, the different methodologies used to deliver SIA, as well as of the perceived benefits and potential barriers to successful SIA. In the second session, a structured guidance for SIA (developed by the colleagues at Trilateral Research and Consulting) was presented. It focused on the question of how to put implement SIA in practice and of how to

construct an SIA report, with an emphasis on 'best practice' criteria and principles. This session also provided insights into the possible organisational and structural ramifications of SIA, arguing that SIA should not be considered as a process isolated from the rest of the project (and project design). A third session aimed to share experience from doing SIAs in the context of public transport, to help participants to develop an understanding of how an SIA should be integrated with existing organisational procedures and how existing institutional practices shape the development of an SIA. In this respect, this session demonstrated how any security system needs to be understood in their broader organisational, political and social context. This session also identified critical success factors in the deployment of SIAs.

The second part of the Masterclass consisted of an interactive exercise. Participants broke up into three groups and were given instructions to develop a SIA plan for a project that has been simulated by the ASSERT consortium for the group exercise. Participants were asked to imagine that they are planning to submit a proposal based on the Horizon 2020 topic *FCT-2-2015. Forensic topic 2: Advanced easy to use in-situ forensic tools at the scene of crime*. They were told to be a part of the core group of the consortium and some preliminary ideas for the proposal have already been drafted. These include some ideas for potential consortium partners and potential Work Packages (see Annex IV).

Proposed Research Objective

The main objective of this proposal is to discuss and develop a portable hands-on, rapid forensic tool for DNA analysis to be used by law enforcement agency (LEA) field operatives in different contexts. The data produced using this portable device shall be applicable for different purposes within the realm of law enforcement and criminal justice.

After having received some training on SIAs in the first part of the Masterclass, participants were tasked with developing a SIA plan for this proposal/project, and to revise the overall structure of the proposal and consortium if necessary. They were told that all elements of the draft could be reworked and adapted, and that work packages and consortium partners could be added or deleted if necessary.

The groups were told that the expected outcome of the group exercise was to:

- Review and adjust (if necessary) the proposal and the consortium;
- Develop an appropriate SIA-plan, including a working plan and a description of the processes.

Finally, participants were asked to present the findings of the work in a short, 15 minutes presentation, focusing on:

- SIA procedures applicable in the project;
- Impact of SIA plan on the project design (design, process, consortium);
- The societal impacts that this project is likely to create;
- Produce a graphical representation displaying inter-relationships between the different work packages with special emphasis on SIA.

4.2 The Masterclass Group Exercise Results

The Masterclass group exercise was kicked off by an introduction that set out the activities to be undertaken during the ASSERT Masterclass SIA Group Exercise, including: proposed timeframes, key activities, and expected outputs. The groups were then introduced to the task and the schedule for the afternoon. Groups were asked to look at the rough draft of the Work packages and ideas for their project, develop an SIA plan and consider the organisation of the project, the consortium and scope that the SIA would have, and deliver a 15minute overview of the outcome of their discussions to the plenary. The main learning objective of the exercise was that participants should obtain a good understanding of how to design an SIA for a European security research project proposal.

The ASSERT consortium members left it to the groups to decide how they wanted to structure their discussions and tried not to interfere in the group work but to merely observe the discussions and to provide assistance when needed. The following section summarises the notes of group work results presentations.

Group 1:

Group 1 started their work with revisiting the consortium and the work package composition. They then decided to add a data protection authority to the consortium. The group also considered including an external ethics advisor to the group, but no final decision was made in this respect. Work package 3 (societal effects of *in situ* technologies) was restructured so as to include a process to identify SIA stakeholders step by step. The process envisaged by the group started with a workshop for consortium members and then moved on to engaging stakeholders and identified further stakeholders. The group emphasised that there should be close cooperation with a public relations consultancy that should feed SIA findings into each WP. The group found that a proper validation of the new technologies was crucial for the consideration of the societal impacts. They identified a number of SIA issues by carrying out a preliminary impact assessment, following the SIA guidance provided by TRI. The results of this were fed into WP3. The group identified some overlap of societal needs and benefits of the project: cost reductions, low level of error, stronger convictions and transparency. Both dissemination and SIA were understood by the group as activities that should accompany the project for its entire duration (and possibly beyond) and should feed back into the work packages. The group then considered the budgetary implications of SIA (both the cost of the SIA itself, as well as the implications for the rest of the budget that findings from SIA may have). Treating SIA as primarily a public relations matter, they argued that the marketing budget should be higher than the management budget to ensure that the evaluations are fed back to the operational aspect of the project.

Group 2:

Group 2 set off with a stocktaking exercise to map societal issues raised by the proposal. After that the consortium and structure of proposal were revisited. The group spent considerable time discussing legal systems, standards and jurisdiction, which led to a

change in the focus of the project. The project was relabelled as a pilot study of five countries as a result, and the proposal was amended to embed the SIA process in the first three work packages. The composition and sequence of work packages were changed to create a feedback loop to WP4 ("Technical Problems"), in order to repeat the SIA process twice. The technological development tasks were estimated to raise new issues and to feed back into the SIA process. The group revised the dissemination plan – they expected it to be difficult to establish a dissemination strategy for 28 countries. Part of the dissemination WP became therefore the development of an implementation template that all countries could adopt and amend to suit their own specific needs. The group also found that the SIA guidance could be embedded in WPs 1-3. Consultation with the most important stakeholders was considered crucial here: harvesting expert knowledge; an advisory board that 'balances the narratives'; identifying important stakeholders, especially NGOs that deal with offenders, penal reform, resettlement of offenders; engage regulators from the EU member states. The group also envisaged installing an active advisory group to organise regular consultative meetings with all relevant stakeholders.

Group 3:

Like the other groups, Group 3 started its work with a discussion of the scope of the project and the consortium. They decided not to change focus of the project. Planning the SIA process, the group allocated some 5 per cent of the budget towards SIA activities and appointed an academic partner of the project as leader of SIA-related tasks. Regarding the structure of WPs, WP3 ("Societal Effects of in-situ Technologies") was redesigned to be a work package on legal and ethical issues. The group emphasised that the SIA process should be an integral part of each WP. SIA should also entail a public dialogue and be as transparent as possible. The group also envisaged the recruitment of the stakeholders of the SIA process to take place in three steps:

1. open call for stakeholder engagement;
2. an ongoing call for participation across the project;
3. active recruitment - consider stakeholders we want / believe need to be included;

The use of social media was considered crucial for awareness-raising for the SIA, and for encouraging participation. Different methods were discussed for organising the SIA process, and focus groups were considered to be particularly helpful. Finally, the group discussed whether or not there should be the possibility to abort the project when certain criteria are fulfilled. The group members then suggested and agreed on a 'stop and go approach', with decisions at each stage as to whether or not the project would proceed, or the development would be halted.

While no systematic feedback was given to the participants after the group work presentations, a look at the group work along the good practice principles allows identifying challenges in implementing them. In future Masterclasses we will aim to provide structured feedback to groups, drawing upon the observations and notes of the observers/moderators in each group (who would be members of the ASSERT consortium):

Good practice criterion	Group 1	Group 2	Group 3
Change	All groups considered the consortium composition and the work plan as objects of change. This shows the difficulty to amend the objectives in pre-determined calls		
Participation	A step-by-step approach for identifying stakeholders was envisaged	Compared to the other groups, a rather conventional mode for participation was envisaged, this group saw a major role for the advisory board to 'balance narratives'	A step-by-step approach for identifying stakeholders was envisaged, including an ongoing call for invitations to participate
Flexibility	Flexibility was primarily understood in terms of iterative processes.	Flexibility was primarily understood in terms of iterative processes.	This group considered the highest level of flexibility by discussing 'breaking points' that could lead to the abortion of the projects
Iteration	All groups considered iteration as crucial, they understood it as the constant feedback of the SIA results into the R&D process. This highlights the difficulty to clearly separate the R&D process from SIA processes.		
Administrative Burden	The administrative burden was primarily considered as a budget issue by all three groups		
Transparency	The issue of transparency was primarily understood as a way of communicating what is being done in the project to consider societal impacts	This group considered transparency as an issue of 'marketing' the project and product	The issue of transparency was primarily understood as a way of communicating what is being done in the project to consider societal impacts. An emphasis was put on the use of social media to create transparency
Limitations	This group saw the limitations of the SIA within the objectives of the project	This group saw the limitations of the SIA within the objectives of the project	This group saw the limitations of the SIA as very wide by considering to abort the project if certain conditions are met
Societal Security	Societal security was not discussed in the presentations of all three groups. This is probably due to time restraints of the presentations, as the observers of the group work confirmed that societal security issues have been discussed in the work sessions. This result hints at the need to better operationalise societal security for SIA		
Societal Impact	Interestingly, all three groups focussed their presentations on technical and methodological aspects of SIA. Societal impact was not discussed in detail. This hints at a conceptual problem to plan a process for issues that are not yet known but can only be imagined.		
Knowledge Type	All three groups considered the knowledge procuded by SIA as both important for decision making and managing as well as for the R&D process itself.		

Table 2: Overview of Masterclass group work results structured along good practice principles. (This table will be revised further following the results of discussions at the 2nd ASSERT Masterclass on 29 April 2014).

The discussion following the group work presentations

The ensuing discussion revolved around the question of how SIA changes the ways that security research on the European level is being done. Technically, it is unclear whether or not the European Commission expects H2020 project proposers to include a work package dedicated to SIA . Another question that created a lot of discussion was what kind of budget should be considered reasonable for SIA. Consultative processes are costly endeavours, and can increase the overall budget for research projects considerably. Furthermore, the discussion revealed difficulties in clearly distinguishing SIA activities from R&D activities. It was felt that even in technological development, SIA should be an integral part of the research process. It became clear in the discussion that the overall concepts for SIAs and the methods to implement SIAs largely depend on social science expertise.

Whether or not the possibility to abort projects should be an option arising from SIA was a contested issue in the discussion. Participants in favour of this option argued that it could lead to a better consideration of 'break points' for R&D projects. It was argued that the insight that a particular project was unfeasible, or unacceptable from a societal impact standpoint, was an important potential result from SIA, and that the documentation of such decisions should be supported. Documenting unsuccessful paths, they argued, could help to save large amounts of research money later on. Making the definition of break points mandatory at least for projects and programmes that have been labelled as critical in a threshold analysis could become an issue for future lobbying activities. Some researchers in the security sector are currently considering the launch of a lobby group to promote the societal security concept and the value of SIA.

The detailed prescription of the outcome of security research calls was widely perceived as an obstacle for SIA because it limits the flexibility that is often needed in research projects. One participant called for an understanding of societal impacts as a creative challenge. Such an understanding could be promoted by conducting SIAs of funding calls before they are published – an idea that was raised also during the Berlin workshop. Some participants were against this, arguing that there should be as many opportunities as possible to do research projects, especially when there are SIA procedures in place to manage the societal impacts, and that the scope of acceptable research should not be limited beforehand. Viewed from this perspective, it became clear that SIA bears the danger of restricting research in ways that are seen as counterproductive by some actors.

On a methodological level, one participant said that what had been missing in the group work presentations had been the role of the mass media in the promotion of SIA. Another issue that had not been addressed was the inclusion of vulnerable groups as stakeholders in SIA processes. A participant seconded that if vulnerable groups are included into stakeholder engagement, it alters the ways that ethical reviews are being done (i.e. in some countries the inclusion of vulnerable groups in the project in any capacity would render the ethics approval much more difficult). This discussion then turned towards the type of consultation that should be underlying SIAs. While there is a possibility of spoilers or 'professional victims' to troll SIA processes, a participant emphasised that consultations are not just about speaking to people but about giving them a voice and showing them how they can change the ways that projects are being implemented.

At the end of the session discussions focused on the degree to which certain elements of SIA – documents, standards, procedures – should be made a mandatory requirement. One participant was sceptical towards the inclusion of any kind of mandatory measures due to questionable enforceability in this context; the participant pointed out that there already are a lot of guidance documents and people often do not read them. Another participant emphasised that the failure to acknowledge SIA as an evaluation criterion might have the effect that proposals with good SIA plans might appear too complicated to deliver. Many participants supported the idea of scoring SIA plans in the evaluation process. This would, however, require making explicit and very clear what exactly SIA were expected to deliver in future research calls.

Participants also discussed the merits and limits of a one-size-fits-all approach towards SIA. They widely agreed that there is place for both 'mini' and 'maxi' SIAs, depending on the phase of the project, and depending on the societal issues at stake. A flexible approach that is informed by good practice criteria without being overly formulaic was seen as the best approach towards giving SIAs a role in the RRI framework.

4.3 Lessons learnt from the Masterclass

This section draws on the final discussion of the Masterclass and on the results of a formal feedback questionnaire that was turned in by 16 participants. Reflecting the learning outcomes, participants felt that:

- SIA is becoming increasingly important and that it will be a crucial issue in the future;

- SIA is an intrinsically political process;

- Because of its political nature, there is no one size fits all approach to SIA;

- It seems reasonable to assume that in five years' time SIA will be a mandatory part of research proposals, in the same way that ethical reviews are today. There is now an opportunity to shape how SIA will be done in the future;

- In absence of a detailed model, it is important to understand the critical success factors – pitfalls, barriers to delivery of a SIA.

Participants at our first Masterclass found that the conceptual introductions and the presentation of the guidance paper were useful for the preparation of the group work. They also appreciated the group learning exercise. While the participants emphasised that the social activities organised around the Masterclass contributed to the successful learning experience, they also said that it would have been good to create a more heterogeneous group, including policy makers and technology developers. Other participants said that the group work would have benefitted from group compositions that resembled the compositon of real-world project consortia.

The ASSERT consortium concludes that a crucial challenge for the refinement of the Masterclass-concept lies in the partly contradictory requirements that are structurally embedded in the SIA concept. On the one hand, there is a strong demand for step-by-step guidance and instructions. On the other hand, participants acknowledged the difficulties of blueprints and expressed a strong demand for discussions, reflection and learning. One way to deal with this contradiction could be to include a session in the

Masterclass where learning from a real historical SIA case (practice example) takes place. This would include the presentation and discussion of a 'how-to' recipe on the conceptual level, and how this recipe can then introduced in practice. This session should be followed by sufficient time for discussion.

5. Harvesting existing methods and approaches

This section documents a number of important projects and documents featuring methods that reflect the state of the art of SIA in security research. The list is not comprehensive. Instead it is an annotated collection, highlighting the contribution of these projects to ASSERT's objectives. It also responds to a request by several participants in ASSERT activities to collate an overview of SIA-relevant sources and materials.

5.1 Projects

The EST framework project (http://estframe.net/) is an effort to integrate the RRI and SIA discourse. It organizes a series of stakeholder workshops at the European level, which are an important extension of ASSERT's efforts in this regard. While no substantial results have been published so far, the EST project should be integrated in efforts following up on ASSERT.

Closely related to EST, the EPINET (www.epinet.no) project studies innovative approaches to impact assessments in four technology areas, namely wearable sensors, cognitive technical systems, synthetic meat, and smart grids. EPINET's focus is on promoting the concept epistemic networks as a way of 'conceptualizing complex developments within emerging fields of sociotechnical innovation'.

The PACITA project has established a technology assessment platform at a European level: http://www.pacitaproject.eu/. Not limited to security research, PACITA promotes efforts for 'evidence based policy making', 'public engagement in science', scientist-stakeholder communication, and ethics. Innovative approaches do not feature prominent in PACITA, but it is a widely recognised platform for established technology assessment procedures.

The CIVISTI project (www.civisti.org) has developed a participatory methodology for participation in the planning of research and development methodology. It features a three-stage process, where citizen consultations first produce visions for the future, experts then transform those visions into research recommendations, and citizens finally validate and rank the recommendations. This methodology has potential for application in the security R&D program planning phase. Interestingly, security was not included in the remit of the project.

Another contribution from the Scandinavian research community is the DoingForesight project (www.doingforesight.org). This project has developed a web-based application to to aid the anticipation and evaluation of social impacts. The tool has a generic approach to R&D projects and would need to be adopted for use in the security R&D domain – a problem that is often encountered with tools that tend to be either too generic or too specific to be transferred from one domain to another without requiring large amounts of additional work.

The DESSI project (http:// http://securitydecisions.org) has developed a tool to aid decisions about investments in security technologies. More precisely, the tool consists of a participatory methodology for impact assessments and a web-based tool to document and manage the process and results. The tool does not cover the whole R&D phase, but it focuses on decision-making in the implementation of security technologies and measures.

Similar to DESSI, the SIAM project (http://www.tu-berlin.de/ztg/menue/forschung/projekte_-_laufend/security_impact_assessment_measures_siam/) has developed a tool for assessing societal impacts of security technologies. The SIAM tool requires the adaption of a database of assessment criteria and questions for assessments. It provides consultative assessment process guidance and documentation.

The PRISE project (http://www.prise.oeaw.ac.at/) has 'provided assistance to the European Union in shaping forthcoming security research programmes in accordance with its fundamental values'. It did so by developing criteria and guidelines that were designed to support security R&D that is compliant to fundamental values. The scope of PRISE is limited due to its legalistic character and a lack of mechanisms that support the use of the criteria and guidance.

The SURPRISE project (http://surprise-project.eu) focuses on the relationship between security and privacy. It investigates citizens' opinions on wide-spread surveillance end technological security. Like ASSERT, it operates with the notion of societal security.

The TAMI project (http://www.ea-aw.org/research/archive/completed-projects/tami.html) developed typologies of impact of technologies, but was not specifically concerned with security technologies. However TAMI's broad temporal scope, encompassing the whole lifecycle of a project beginning with planning and ending with implementation, is an important predecessor for ASSERT.

The TASTI project (http://www.spiral.ulg.ac.be/fr/recherche/science-technologie-et-societe/projets-pole-sts/tasti/) project is an attempt to map the societal entanglements of research and innovation, using a broad set of different methods. With its focus on societal entanglements, it is a relevant contribution to the overall approach of SIA promoted in ASSERT.

The SIAHUB platform (http://www.socialimpactassessment.com) is a platform for networking and assessing resources in SIA.

The RESPONSIBILITY project (http://responsibility-rri.eu) is concerned with the development of a Global Model and Observatory for International Responsible Research and Innovation Coordination. Especially the transnational scope of RESPONSIBILITY is a very important extension for ASSERT that should be considered in follow-up actions.

Also national efforts to consider the societal dimensions of security research have emerged. These are, however, rarely recognised on the European level. It would be crucial to map those programs, to evaluate them and to integrate them into the European discourse. Recognising how European and national efforts overlap could lead to a more effective support for SIA.

5.2 Documents & Methods

In the last FP7 security calls for proposals, the EC included a societal impact assessment table in the proposal template. While it was a requirement to fill in the table, the content was not evaluated. The table is the result of a consultative process with a group of experts that included representatives from NGOs. This table and the questions are the resources that come closest to an official specification of how societal impact could be understood in security research:

Ensuring security research meets the needs of society

Which documented societal security need(s) does the proposed research address?

How will the research output meet these needs? How will this be demonstrated? How will the level of societal acceptance be assessed?

What threats to society does the research address? (e.g. crime, terrorism, pandemic, natural and man-made disasters, etc.).

How is the proposed research appropriate to address these threats?

Ensuring security research benefits society

What segment(s) of society will benefit from increased security as a result of the proposed research?

How will society as a whole benefit from the proposed research?

Are there other European societal values that are enhanced by the proposed research e.g. public accountability & transparency; strengthened community engagement, human dignity; good governance; social and territorial cohesion; sustainable development etc.?

Ensuring security research does not have negative impacts on society

If implemented, how could the research have a negative impact on the rights and values enshrined in the Treaties (e.g. freedom of association, freedom of expression, protection of personal dignity, privacy and data protection etc.)?

If implemented, how could the research impact disproportionately upon specific groups or unduly discriminate against them?

What specific measures will be taken to ensure that the research outcomes comply with the European Charter of Fundamental Rights and to mitigate against any of the negative impacts described above?

Source: FP7 Security Research Proposal Template

This table provides a good starting point for SIA in the proposal preparation phase. The European Commission should do more to raise the awareness in the research community that what is written in the table is considered important for the consideration of impact in the review process. Furthermore, the European Commission should provide evaluators with guidance for evaluating the content of the societal impact table in order to increase the coherence of the way it is understood. The good practice principles for SIA outlined in this Report could be used for this purpose. The set of questions in the table should be amended by questions about what measures are being taken to anticipate, and to avoid if necessary, negative social impact during the course of the project. The current legalistic reference to the European Charter of Fundamental Rights is too abstract and at the same time not broad enough.

It should also be added that the European Commission has an impact assessment procedure in place that is, however, currently limited to the realm of EC policy making. It requires Directorates to carry out impact assessments for any policy proposals within their domains.[14] The guidance sets out a roadmap consisting of nine steps that lead to the production of an impact assessment report:

1. Planning of Impact assessment (IA): Establishing the need for an IA. Roadmap drafting and publication.
2. Setting up an IA steering group: Involving all relevant Commission services in the preparation of the IA.
3. Consulting interested parties, collecting expertise and data.
4. Carrying out the IA analysis.
5. Presenting the findings in the draft IA report.
6. IAB (783 kB) scrutiny and recommendations (opinion) on the draft IA report.
7. Revised IA report & IAB opinion(s) go into inter-service consultation along with the draft proposal.
8. IA report, executive summary, IAB opinion(s) & proposal submitted to College of Commissioners.
9. Final IA report, executive summary & adopted proposal transmitted to other EU institutions and published on Europa (783 kB) .

The guidelines contain tables with categorised questions to facilitate the assessment of social impact. Economic, social, and environmental impacts are treated as separate categories. For assessing social impacts, eleven sets of questions are provided, covering:

1. Employment and labour markets
2. Standards and rights related to job quality
3. Social inclusion and protection of particular groups
4. Gender equality, equality treatment and opportunities, non - discrimination
5. Individuals, private and family life, personal data
6. Governance, participation, good administration, access to justice, media and

[14] http://ec.europa.eu/smart-regulation/impact/commission_guidelines/commission_guidelines_en.htm [last access on April 23, 2014]

ethics
7. Public health and safety
8. Crime, Terrorism and Security
9. Access to and effects on social protection, health and educational systems
10. Culture
11. Social impacts in third countries[15]

The guidance document emphasises that assessing these social impact dimensions requires qualitative data collection and analysis. Regarding the analysis, a two-step process is outlined to identify "more important" dimensions on which the subsequent analysis should focus. The document also refers to further guidance for social impact assessment provided by the Directorate for employment, social affairs & inclusion.[16] Here, emphasis is placed on assessing the impact of policies on employment, adequate social protection, education and training, and the protection of human health with the objective to eliminate inequalities, fight discrimination and social exclusion, and to promote gender equality. While it is beyond the scope of this Deliverable to review these guidance documents in detail, the approach of the document towards identifying social impacts resonates with the good practice criteria proposed by ASSERT: ultimately, the societal impact of a policy or project or product needs to be determined in the course of the formulation and implementation by the people who run the project. The high ambitions of the European Commission's guidance for impact assessment pose major challenges for implementation. Lee and Kirkpatrick (2006), in a study of impact assessments following European Commission guidelines from 2003, concluded that

> *In several respects, current EC guidance on integrated impact assessment is already well- founded and helpful but there are some possible gaps (for instance, relating to the usefulness of a non-technical summary) and some points where additional clarification and emphasis might be helpful. Also, previous experience in impact assessment training suggests that practitioners can benefit from systematically assessing (for themselves) the quality of the kinds of impact assessments in which they and their colleagues are likely to be directly involved. In this way, the lessons to be drawn from quality reviews, undertaken by those engaged in the assessment process, may be more easily digested.* (Lee/Kirkpatrick 2006: 32)

While the new guidance from 2009 yielded great progress towards clarifying the terms and concepts and detailing how to an impact assessment, it is unclear whether or not efforts have been made to provide for more hands-on training. It is here where ASSERT can make a valuable contribution with the Masterclass concept. The commission conducted an impact assessment for the Horizon2020 research programme, framing

[15] http://ec.europa.eu/smart-regulation/impact/commission_guidelines/docs/iag_2009_en.pdf, pp. 35-36.
[16] http://ec.europa.eu/social/main.jsp?catId=307&langId=en [last access April 23, 2014

research and innovation as "key engines of productivity and growth".[17] The societal impact of H2020 is therefore primarily discussed in terms of its contributions towards a sustainable economic growth in Europe and the competitiveness of the European industry. The report acknowledges the different perspectives of stakeholders, comprising the industry, academic institutions, and public organisations and government bodies on European research policy making. While the industry has an interest in simplification and on support for innovation, academic institutions emphasize the importance of both applied and basic research, specifically for research on societal challenges. Government bodies have expressed their interest in a European framework for research and innovation. Technically, a central argument in the report is that evaluation should be a process rather than a one-off exercise, and that results from the evaluation should feed into R&D processes. In this regard, the European Commission's approach towards impact assessment bears some similarities with ASSERT's approach towards an iterative SIA procedure.

Reading through the Commission guidelines, the ambitious approach of the documents is likely to exceed the capacity of policy planners and research to comply with the guidance. It is therefore important to manage what Sutcliffe, reviewing the RRI policy discourse in European R&D (2012), called "conditions of uncertainty and ignorance" in an open and transparent way. His recommendations are is in line with some of the best practice criteria. They provide an example of how the impact assessment discourse overlaps with the discourse on RRI, and how the two can enrich each other:

- *Governments sharing their innovation strategy and the trade offs and assumptions they have made with all citizens*
- *Governments taking steps to communicate clearly about how decisions are made about the research and applications of innovation and how the public interest has been embedded*
- *Feedback to participants in dialogues about how their views influenced the decision making process*
- *Businesses being open about their use of new and controversial technologies in their products. At what stage in the research process this happens is moot because of concerns about IP, but as products are brought on to the market then this should be made clear, if not before. This is currently not the case, for example with nanotechnologies.*
- *All actors being honest and open about the potential benefits in the round and the potential negative impacts of their use of a technology and their solutions.*
- *All actors opening up about the processes they have undertaken to ensure that the product or technology is safe for the public or the environment.* (Sutcliffe 2012: pp.17)

While this list is by no means comprehensive, it emphasises the importance to think SIA as not taking place in a vacuum, but contingent on organisational cultures, national borders, and bureaucracies. The ASSERT Masterclass represents an attempt to provide training that increases the capacities of academics and practitioners carrying out SIAs

[17] http://ec.europa.eu/research/horizon2020/pdf/proposals/horizon_2020_impact_assessment_report.pdf [last access April 23, 2014]

to contextualise impact assessment procedures.

6. Summary: Taking SIA in security research to a new level

This Deliverable set out to define good practice principles for SIAs in security research, and demonstrated how these principles can be used to plan and to assess SIAs in different phases of the R&D process. These good practice principles seek to enhance the potential of SIA processes to modify the goals, categories, and methodologies of the project, and they concern the depth and level of consultation and participation, the flexibility, transparency and iterative nature of the process, the proportionality of the administrative costs incurred by SIA, and the clarity about the goals, limitations, and about the kind of knowledge produced by a specific SIA process (see also Appendix 1).

Furthermore, the Report introduced a format for SIA training (ASSERT Masterclass) and discussed ways to improve the format on the basis of feedback from participants in the first Masterclass in February 2014. A major challenge for these training events continues to be striking the right balance between the demand for detailed step-by-step instructions and blueprints on the one hand, with the necessity to avoid an over-determination of the outcome and appearance of the SIA process on the other. This challenge stems from the fact that SIA are prospective in nature and thus are inevitably shaped by issues that cannot be anticipated beforehand.

7. References

Harvey, B. (2011). Foreword: SIA from a resource developer's perspective. In: Vanclay, F., and Esteves, A.M. (eds.) New Directions in Social Impact Assessment: Conceptual and Methodological Assumptions. Cheltenham: Edward Elgar. xxvii-xxxiii.

Wadhwa, K./Barnard-Wills, D./Wright, D. (2014). State of the art societal impact assessment for security research. Unpublished paper. London.

Bogner, A. (2012). The paradox of participation experiments. Science Technology and Human Values 37, 5, 506-527.

Beck, U. (1992). Risk society: towards a new modernity. London: Sage.

Buzan, B./Waever, O./Wilde, J. (1998). Security: A New Framework for Analysis. Lynne Rienner Publishers.

Cashmore, M. (2004. The role of science in environemtnal impact assessment: process and procedure versus purpose in the development of theory. In: Environmental Impact Assessment Review, Vo. 24, 403-426.

CIES (2012). Report of the Societal Impact Expert Working Group. Available online at [http://www.pol.gu.se/digitalAssets/1363/1363359_report-of-the-societal-impact-expert-working-group-2012.pdf] [28.02.2014].

EC (2013). Options for Strengthening Responsible Research and Innovation. Brussels. Available online at [http://ec.europa.eu/research/science-society/document_library/pdf_06/options-for-strengthening_en.pdf] [28.02.2014].

ETTIS (2012). A Working Definition of Societal Security. ETTIS Deliverable D1.2. Available online at [http://ettis-project.eu/wp-content/uploads/2012/03/D1_2.pdf] [28.02.2014].

Eurobarometer (2013). Responsible Research and Innovation (RRI), Science and Technology. Special Eurobarometer 401. Available online at http://ec.europa.eu/public_opinion/archives/ebs/ebs_401_en.pdf] [28.02.2014].

Hayes, B. (2009). NeoConOpticon: The EU Security-Industrial Complex. Available online at [http://www.statewatch.org/analyses/neoconopticon-report.pdf] [28.02.2104].

IRISS (2012). Surveillance, fighting crime and violence. IRISS Deliverable D1.1. Available online at [http://irissproject.eu/wp-content/uploads/2013/04/Surveillance-fighting-crime-and-violence-report-D1.1-IRISS.pdf] [28.02.2014].

Kreissl, R. et al. (2014). Societal Impact Assessment. Contribution submitted for the International Encyclopedia of Social and Behavioral Sciences.

Lee, N./Kirkpatrick, C. (2006): Evidence-based policy-making in Europe: an evaluation of European Commission integrated impact assessments. In: Impact Assessment and Project Appraisal, Vol. 24 (1), 23–33.

Mol, A. (2003). The Body Multiple: Ontology in Medical Practice. Durham: Duke University Press.

Nuffield Council on Bioethics (NCoB) (2012). *Emerging Biotechnologies*. London.

Prainsack, B./Toom, V. (2010). The Prüm regime: Situated dis/empowerment in transnational DNA profile exchange. In: British Journal of Criminology, Vol. 50, 1117-1135.

Prainsack, B./Ostermeier, L. (2013). Report on methodologies relevant to the assessment of societal impacts of security research. ASSERT deliverable 1.2. Available online at [http://assert-project.eu/wp-content/uploads/2013/04/ASSERT_D1.2_KCL_final.pdf] [28.02.2014]

Prainsack, B. (2014). Understanding Participation: The 'citizen science' of genetics. In: Barbara Prainsack, Silke Schicktanz, and Gabriele Werner-Felmayer (eds). Genetics as Social Practice. Farnham: Ashgate (in press).

Rappert, B. (2012). How to look good in a war. Justifying and Challenging State Violence. London: Plutopress.

Sutcliffe, H. (2011): A report on Responsible Research & Innovation (On the basis of material provided by the Services of the European Commission. Prepared for DG Research and Innovation, European Commission). http://ec.europa.eu/research/science-society/document_library/pdf_06/rri-report-hilary-sutcliffe_en.pdf [last access 23 April 2014]

Vanclay, F. (2003). International Principles for Social Impact Assessment. In: Impact Assessment and Project Appraisal, Vol. 21, No. 1, 5-11.

8. Annex

Annex 1: The ASSERT Good Practice Criteria for Societal Impact Assessments

1. Clarify how societal security is understood in a given project (especially when this is implicit).

How does the project enhance the security of European citizens and societies?

Whose security?

2. Clarify how societal impact can be operationalised in the context of a particular project.

What questions do you need to ask in order to find out what, how, and when factors will likely impact society?

Impacts can include any kind of benefits, unintended consequences, harm, on individuals, households and enterprises and communities

Avoid looking for technological "fixes" for societal problems

3. Give the SIA design the potential to reframe the project and R&D process.

Modification of goals, categories and methods

Threshold analysis

4. Take participation seriously. 'Participation' of relevant people and groups means more than merely to inform or consult them.

How can this be established (agency assessment)?

Who is in the position to define what is important and less important?

Are the roles and responsibilities clearly defined?

5. Make sure that the SIA process is flexible.

What level of flexibility is productive?

Adapt and adjust to new evidence, new insights, or changes

6. Create feedback loops between SIA and the rest of the project / programme.

Where in the R&D process does SIA create an impact?

7. Keep the administrative burden reasonable.

Redesign existing assessment processes that are already in place

What is reasonable depends on the project

8. Think about transparency and the limitations of the SIA process.

Are there situations where transparency cannot or should not be achieved?

Limits of temporal and geographical scope; budget etc.

9. Clarify what purpose the knowledge produced in a SIA should serve.

Do you want to use it primarily within the project itself, to make the project more socially robust?

Do you want to use it to communicate with policy makers?

Do you need it for an evaluation report?

Annex 2: Societal Dimensions in Eurobarometer

- Science and Tech make life easier, more comfortable and healthier
- Science and Faith
- Creates more opportunities for future generations
- Speed of change in science and technology
- Science and Technology can threaten human rights
- Most think that fundamental rights and moral principles should not be violated to make a new scientific or technological discovery
- A large majority agree that the EU should promote the worldwide respect of European ethical principles
- More than three quarters of respondents agree the EU should take measures to address the ethical risk of new technologies
- Most agree that respecting ethics and rights guarantees research and innovation will meet citizens' expectations
- A large majority think there should be mandatory ethics training for researchers, and an oath taken to respect ethical principles and legislation

- At least eight in ten agree that scientific experts should be transparent about their sources of funding
- Most agree that an interest in science improves young people's job prospects, culture, and their ability to act as well-informed citizens
- A large majority think the needs of men and women should have equal weight in scientific research
- The majority agree that the results of publicly funded research should be available online for free

Annex 3: Agency Assessment Guidance

Grid to help to assess the agency of public participants in impact assessment projects. Adapted from Prainsack (2014).

Coordination: Who has influence in:

1. Agenda setting

2. Determining the terms of the execution of the idea/procedural aspects

3. Deciding what results are (and what 'good' results are)

4. Deciding what will be done with results

5. Deciding on intellectual property questions

Participation

6. Who participates (demographic and social parameters of those who participate)? Why, and how do they participate?

7. How much, and what kind of, training, skill, or expertise is required to participate in this project?

8. Are there cultural, institutional, or other differences in perception and framing of core issues and stakes?

Community

9. What forms of community pre-exist this project, if any? Which new communities does the project facilitate or give rise to? What is the constitutive factor for the feeling of belonging on the side of the participants?

Evaluation:

10. How and who decides what good outcomes are?

11. What happens to the results of these evaluations?

Openness and information symmetry:

12. Do participants in the project have access to the core data about the project?

13. Can participants in the project edit/change the core datasets?

14. Is the contribution of participants adequately acknowledged in published materials, and policy briefing documents, etc?

15. Are datasets made publicly accessible (open source/open access)?

16. Are main findings made publicly accessible (open source/open access)? Are assessment reports made publicly accessible?

Entrepreneurship:

17. How is the assessment project funded?

18. What is the role of for-profit entities in this assessment project? Are these small, medium-sized, or large entities, and where are they located?

19. How are for-profit and other interests aligned in this assessment project (and/or do they conflict, and where?)

Annex 4: Call topic, Work packages, tasks, and consortium for the Masterclass group exercise

Call Topic: FCT-2-2015. Forensic topic 2: Advanced easy to use in-situ forensic tools at the scene of crime

Specific challenge:

Rapid developments in technologies and communication in various fields go hand in hand with new opportunities for forensic science to investigate more and a greater variety of traces, to extract more information from less material, quicker than ever before, and to keep the standards of forensic science in Europe at a high level regarding juridical and technological questions. Meanwhile, organised crime and criminals do not limit themselves to regional or national borders. Their crimes are thus leaving traces in multiple countries. Cross border access to evidence has become an absolute necessity for Law Enforcement Agencies (LEA) and judicial authorities.

Evidence gathering, collection and exchange at EU level should be usable from the field to the judge, independently of where the crimes have taken place. Rapid developments in technologies and communications in various fields go hand in hand with new opportunities for forensic science.

Proposals for this topic should take into account the existing EU and national projects in this field, such as the Council Conclusions on the vision for European Forensic Science 2020 which foresee the creation of a European Forensic Science Area and the development of forensic science infrastructure in Europe."

Scope:

Proposals for this topic should focus on the development methodologies of tools and EU-wide standards for the secure storage, access and the exchange of forensic data supporting evidence.

A platform integrating different techniques should be proposed in order to achieve better strategies for gathering evidence in the field of forensic research. Relying on knowledge- based fields such as artificial intelligence, machine learning, different procedures, tools and algorithm should be developed within this platform, based on the standard outlined above.

Specific areas of research could be:

- The establishment of a EU-wide database of new synthetic drugs and drug precursors (detection protocols and analysis methodologies).

- Other types of pan-EU databases - like for instance soils, ballistic data, breath analysis, DNA, fingerprints, etc.

In addition due to the variability and the wide range of crime types, procedures or methodologies should be developed or adapted to the specific crime features. Moreover, horizontal strategies could be proposed for profiling crimes or offenders and matching and predicting different type of crimes. This should lead to the establishment of a catalogue of these procedures or methodologies.

Where necessary new technologies should be developed for sampling, analysing, evaluating, interpreting and recording forensic evidence, with a view to achieve solid and court-proof forensic evidence that can be used during legal prosecution.

The use of the most advanced information technologies should allow improving and upgrading the current forensic systems in the European police institutions. The scope of the proposed tool should involve law enforcement bodies from the design phase to the prototyping and test phase.

Proposals addressing this topic may involve the use of classified background information (EU or national) or the production of security sensitive results. As such, certain project deliverables may require security classification. The final decision on the classification of projects is subject to the security evaluation. The Commission considers that proposals requesting a contribution from the EU of between €9m and €12m would allow this specific challenge to be addressed appropriately. Nonetheless, this does not preclude submission and selection of proposals requesting other amounts.

Expected impact:

Projects under this topic should lead to the development of novel easy to use in-situ forensic tools, customised to the specific needs of EU LEA. Better profiling of crimes and offenders. Quicker matching of different types of crime. Shorter court cases due to the availability of more solid court proof forensic evidence. For industry better understanding of modern operational LEA requirements, thus increasing their competitiveness. Considerable improvement in the field of public security and improved trust of the citizen in the work of police forces in the EU.

Type of action: Innovation Actions

Proposed Work Packages and Tasks

Work Package 1: State-of-the-Art

Task 1.1 Collect and analyse national and international (European) organizational and administrative frameworks for the collection and use of forensic DNA data in the domain of LEA.

Task 1.2 Review existing methodologies and tools available to collect, store and process forensic DNA data.

Task 1.3 Investigate problems of compatibility and analyse existing interfaces for different systems.

Task 1.4 Develop a comprehensive account of existing regulatory frameworks governing the collection, storage, processing and use of forensic data at national and European levels.

WP 2: Investigate Operational Problems

Task 2.1 Analyse the operational pathways for forensic DNA data. Investigate how the information collected in situ is processed from the place of use of the device (e.g. crime scenes, custody suites) to prosecutors to courtrooms in different countries.

Task 2.2 Investigate how forensic DNA data collected in different situations (e.g. custody suites and crime scenes) can be used for law enforcement purposes.

Task 2.3 Investigate the effects of different storage media on the quality and usability of forensic DNA information.

WP 3: Societal Effects of in-situ Technologies

Task 3.1 Investigate potential discriminatory effects and biases in forensic DNA databases using information collected in situ.

Task 3.2 Analyse potential external effects of the introduction of portable, hands on rapid forensic tools for in situ use. Develop an understanding of changes in the organization of operational routines of LEA.

Task 3.3 Identify other ethical issues (e.g. de-skilling effects, organizational changes, impact on privacy and data protection) and develop adequate strategies to cope with these problems.

WP 4: Technical Problems (Soft & Hardware)

Task 4.1 Draft technical design specifications for the tool to be developed.

Task 4.2 Screen emerging technologies in the field of forensic DNA data collection.

Task 4.3 Assess the potential of existing technical solutions for improving profiling capabilities.

Task 4.4 Develop a solution for high data quality to prevent degradation.

Task 4.5 Assess the potential for automated data exchange processes of in situ tools.

WP 5: Organisational and Accreditation Problems

Task 5.1 Draft functional specifications for the expertise and competencies necessary to work with the in situ tool.

Task 5.2 Examine the demand for training of law enforcement personnel.

WP 6: Product specifications and building a prototype

Task 6.1 Construct a prototype.

Task 6.2 Test the prototype in a lab setting.

Task 6.3 Implement a test run in different national controlled real world law enforcement settings.

WP 7: Project Management

Task 7.1 Project management meetings

Task 7.2 Coordination of the project

WP 8: Dissemination

Task 8.1 Dissemination Strategy (etc.)

Task 8.2 Etc, etc.

List of Consortium Partners

LEA representatives from 5 Member States (= Stakeholder/end-user)

Applied Biosystems Inc., SAP, (= Industry partners)

Europol, Eurojust (= Stakeholder/end-user)

Law Department from a University (e.g. VUB, LSTS) (= legal experts)

KPMG, Accenture Deloitte (= implementation experts)

Northumbria University Centre for Forensic Sciences (= scientific experts)

Annex 5: FP7 proposal template SIA table

Ensuring security research meets the needs of society	
Which documented societal security need(s) does the proposed research address?	
How will the research output meet these needs? How will this be demonstrated? How will the level of societal acceptance be assessed?	
What threats to society does the research address? (e.g. crime, terrorism, pandemic, natural and man-made disasters, etc.).	
How is the proposed research appropriate to	

address these threats?	
Ensuring security research benefits society	
What segment(s) of society will benefit from increased security as a result of the proposed research?	
How will society as a whole benefit from the proposed research?	
Are there other European societal values that are enhanced by the proposed research e.g. public accountability & transparency; strengthened community engagement, human dignity; good governance; social and territorial cohesion; sustainable development etc.	
Ensuring security research does not have negative impacts on society	
If implemented, how could the research have a negative impact on the rights and values enshrined in the Treaties (e.g. freedom of association, freedom of expression, protection of personal dignity, privacy and data protection etc.)?	
If implemented, how could the research impact disproportionately upon specific groups or unduly discriminate against them?	
What specific measures will be taken to ensure that the research outcomes comply with the European Charter of Fundamental Rights and to mitigate against any of the negative impacts described above?	