INSTITUT FÜR RECHTS- UND KRIMINALSOZIOLOGIE
INSTITUTE FOR THE SOCIOLOGY OF LAW AND CRIMINOLOGY

WORKING PAPER NO. 18

Enhancing the EU's Security Industrial Policy through Societal Impact Assessment?

Florian Fritz

www.irks.at
Vienna, August 2014
ISSN 1994-490X

Fritz, F. (2014) Enhancing the EU's Security Industrial Policy through Societal Impact Assessment? *IRKS Working Paper*, 18, 18pp.

Enhancing the EU's Security Industrial Policy through Societal Impact Assessment?

Florian Fritz

Table of Contents

Figures & Tables

1. Introduction[1]

There is rapidly growing awareness that for security measures and technologies to be seen as legitimate and appropriate, consideration of societal needs and of the impacts that research into new technologies can have on all our lives is required. Such consideration is especially critical for the EU's security market. For security technology research and development, this has never been done in a systematic and consistent manner. In 2013, the ASSERT project[2] set out to explore new pathways for integrating assessment mechanisms and procedures into the Research and Innovation cycle. This paper analyses the concept of societal security in light of the EU's "Action Plan for an innovative and competitive Security Industry" (European Commission, 2012) and highlights in what ways ASSERT can contribute to advancing the role of Societal Impact Assessment in processes related to security *research* (as part of industrial activity). The Action Plan illustrates current thinking about the security industrial market, which not only faces difficulties in terms of barriers and fragmentation (due to complex regulatory landscapes, rules for procurements, compliance requirements and restrictions / particularities in security service provision. It is important to note that the Action Plan approaches the concept of s0cietal security from a twofold perspective:

- The societal *dimension* of the security market as such, which as a distinctive feature sets it apart from other relevant industrial markets;
- The societal dimension of security technologies from the perspective of their research and development process.

This distinction will become clearer in the sections below.

Besides attempting a classification and typology of the European security market and the products and services it involves, the Action Plan also reacts on growing resentment towards security (technology) research (which is seen increasingly as detached from real societal needs and more often than not in conflict with fundamental rights and or people's way of life) by foreseeing a stronger, yet not explicitly spelt out role for procedures that assess the societal impacts of security research and test it against unintended negative consequences of publicly funded research in technology. Regarding the pursuit of Impact Assessment (IA) strategies, it should be noted that the underlying objectives differ considerably among proponents: while the EU's Action Plan intends to

[1] This paper builds on the results of the EU-funded research project ASSERT, a Coordination and Support Action which received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 313062.

[2] ASSERT: Assessing Security Research: Tools and Methodologies to measure societal Impact.

instrumentalise IA procedures in order to safeguard return on investments and foster market development, proponents of a comprehensive approach to security research argue 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 and Ostermeier, 2013, p.5). Such an approach builds on inclusion, participatory mechanisms and is guided by societal security more than by particularistic security concepts.

This paper analyses in what ways the policy guidelines of the EU's Action Plan that only sketch the outlines of measures and approaches could spell out in practice, in light of research results achieved by the ASSERT project, and concludes with reflections for an update of the EU's Security Industrial Policy.

2. The EU's Security Industrial Policy

The EU's "Action Plan for an innovative and competitive Security Industry" (European Commission 2012) is of relevance to security research, because it argues for an installation of Impact Assessment mechanisms at an early stage of the R&D process or even in the phase preceding it. The rationale for having IA mechanisms installed is to achieve acceptance of new security solutions. The Action Plan does not build upon one of IA's main assets: that by inclusion, broader participation and engagement a broader potential for innovation can be tapped into. In its 2012 Action Plan, the Commission names the "strong societal dimension" as one of three distinctive features of the EU's security market:

> "Whilst security is one of the most essential human needs, it is also a highly sensitive area. Security measures and technologies can have an impact on fundamental rights and often provoke fear of a possible undermining of privacy." (European Commission, 2012, p.4)

While it has become rather obvious that security technology has, in some cases, certainly done more than merely provoking fear of possible privacy intrusions, the Action Plan also addresses IA aspects from a perspective that is not primarily interested in fostering more societally relevant security solutions and innovation, but with the aim to "provide to the EU security industry a strong home base from which to be able to expand into new and emerging markets, where in the future major growth for the security market can be expected“ (European Commission, 2012, p.12).

The Action Plan identifies three key features of the security market[3] that determine the three major "problems" of the EU's security market. One of those problems the Action Plan therefore calls "The societal dimension of security technologies“. As part of its strategy to foster competitiveness and innovation of the EU's security industry, the Commission proposes to bring in societal considerations into security industrial processes. This societal dimension, framed as one of the three major "problems" the industry faces[4], sketches the outlines of a longer-standing discourse[5] on how to reconcile security research and technological innovation with societal needs and thresholds of acceptability. Also, as shown in the following, the correlation sought between impact assessment mechanisms and user / citizen acceptance, is not conclusively substantiated.

While the Action Plan addresses aspects of the EU-based security industry on the whole (broadly touching upon the gap between research and market and the fragmented character of security products and services, where procurement predominantly is determined along the boundaries of national jurisdictions), security research is one of the core elements explicitly mentioned.

In the Action Plan, it does not become immediately clear why the societal dimension of security solutions should be a "problem" to the market, or even, what kind of a problem. But reading on, the rationale becomes clearer. It has to do with security solutions not being accepted by the "public". This lack of acceptance causes difficulties on the market:

> "The problems assosciated [sic!] to the societal acceptance of security technologies results [sic!] in a number of negative consequences. For industry it means the risk of investing in technologies which are then not accepted by the public, leading to wasted investment. For the demand side it means being forced to purchase a less controversial product which however does not entirely fulfil the security requirements“ (European Commission, 2012, p.5).

Public acceptance, in this logic, is a key factor in making sure investments are not wasted (i.e. not bought or publicly procured[6] or their procurement discontinued due to the experiences made). The "problem" of the "societal dimension" can thus be refined to

[3] The other two being about high market fragmentation along, e.g. national borders, and the "institutional nature" of the security market, which means that buyers are mainly public authorities.

[4] A framing which in itself would deserve closer scrutiny.

[5] e.g. (ESRIF 2009)

[6] Another specifify of the security market is its, in essence, institutional nature, as pointed out in the Action Plan.

the problem of acceptance, which, in turn, determines security (or, rather, efficiency) of investments. This implies a kind of co-existence of two separate strands: one of security-industrial research and development, while the other would be society "out there", waiting to accept or to discard whatever technological solution is deployed. Consequently, the Action Plan positions Societal Impact Assessment (SIA) as an instrument to bridge the gap by fostering an "engineering" of acceptance.

The Action Plan on the EU's security industrial policy envisages such a reconciliation "by thoroughly assessing social impacts including impacts on fundamental rights, and by creating mechanisms to test the societal impact during the R&D phase" (European Commission, 2012, p.6). While such practical considerations certainly are necessary for the further development of societal security, work remains at conceptual level. In principle, what needs to be reconciled is a drive to increase market shares on the one hand and the individual's security from human rights infringements or more general impacts on the social fabric of societies, but also, which should not be overlooked, changed circumstances of everyday life brought about by novel technologies and new ways of deployment.[7]

Way back in 2009, ESRIF postulated that security is about people, society and values (ESRIF 2009, p.13). It would seem a logic conclusion to assume that in order to "reconcile" security technology and measures with society by relating systems, services and products to "people, society and values", SIA could be seen as a promising pathway. Such a process, however, is not a somewhat magical construct of "acceptance engineering", but rather, the process of involving broader segments of society in the innovation and R&D cycle, which, as shown in ASSERT, will work only if SIA processes or mechanisms are taken seriously, most notably because there is the inherent potential of such a process to alter a research project's objectives or lead to a reframing of the problem space as such for which a security solution is to be developed.

3. Impact Assessment as "acceptance engineering"?

The Acton Plan's logic assumes that a "better integration of the societal dimension" of security industrial activities will increase acceptance of its marketed solutions. This, in turn, would guarantee efficiency of investments. To achieve acceptance, Impact Assessments early on in the research process are to be carried out. However, the pathway from assessment to acceptance is far from being linear, and the danger of the

[7] Which, in turn, raises questions of the desireability of solutions to broader segments of society.

process becoming a tokenstic exercise reduced to an attempt at securing legitimacy and good PR are imminent here, unless the void is filled with concrete measures giving SIA the actual power to influence the R&D process in a way that acceptance is a shared feeling in society.

Society, in the Action Plan's logic, is left with a simple choice, being in a position to either accept or reject a security solution. While the Action Plan does not delineate specific factors leading to or inhibiting acceptance, it does propose to remedy such a "bipolar" structure in which a finalised security solution, or a prototype, are subject to a verdict of acceptance or rejection by "the public" before making it to the market. The proposed remedy lies in a "better integration of the societal dimension of security technology". This integration should be realised by creating mechanisms that are able to assess the social impacts of security solutions. The Action Plan does not elaborate on specifics of what such a "mechanism" could look like. In the context of security research, it could have institutional implications, such as the creation of additional expert or advisory groups on "societal impact", and it could also result in a transformation of the research funding programme as such, e.g. by making it obligatory to include a work package on societal impact as early as in the project proposal phase (i.e. before funding decisions are made).

4. The Responsible Research and Innovation (RRI) Agenda

The discussions around (RRI) point in a similar direction. Indeed, RRI could be seen as the broader conceptual framework into which approaches to assessing, measuring or *envisioning* impacts and unintended consequences are embedded.

> "(RRI) refers to the comprehensive approach of proceeding in research and innovation in ways that allow all stakeholders that are involved in the processes 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." (European Commission, 2013, p.3)

As of today, it is rather doubtful whether profound knowledge of the consequences of security research, as well as its unintended consequences caused by research outcomes, are used as "functional requirements" for research and innovation processes of security technologies. The process of involving all stakeholders at an early stage poses specific problems within the security domain, partly attributable to the fact that it is precisely *not* desirable that everyone knows in what specific ways a technology, system or service work because this is what makes it effective, as the argument goes. However, this is in line with the Action Plan's depiction of "testing mechanisms" for societal impact early on in the process.

The testing or assessment of the social impact of security measures and technologies is framed as a tool to ensure acceptance of security measures and technologies and thus to increase or hedge market opportunities. The "locus of intervention" the Action Plan proposes is the "R&D phase", which lends the phase of security *research* prominence throughout the entire process from planning to market.

The causality from impact testing to public acceptance of a marketable solution is not explicated, it is taken as a given. In other words, once such a "testing" has occurred on a proposed research endeavour or on the precursors of a prototype, the proposed security solution is "ready to hit the market". In conclusion, one might suspect that impact assessment is confused for a kind of public relations activity with the overarching goal to create legitimacy; Prainsack and Ostermeier (2013) list several unfavourable scenarios in which Impact Assessment procedures play out as tokenistic or one-off exercises, which, much like with a patient at a doctor's office filling in an informed consent form, still performs the task of creating a certain level of awareness of risks.

The Action Plan does not show clearly in what ways a testing of the societal impact of a research project should enhance acceptance. There are a number of possible underlying assumptions on this causality. One of the least favourable scenarios would be a situation in which being able to show a certificate that demonstrates that a security solution was tested against social impacts, unintended side-effects and ethics considerations (and criteria) might dispel public concerns, thereby – possibly – increasing the likelihood for acceptance. This, of course, would not allow for bifurcations in the research, depriving therefore the Assessment procedure of its potential to alter research outcomes.

In a situation where the results of testing and impact assessment reveal a high likelihood of overwhelmingly negative societal impacts of research, an already on-going research project (the Action Plan explicitly targets the R&D phase) would need to adjust to new parameters in order to converge with impact guidelines. There is a high chance that additional costs would be incurred for the project developers – thus, the original aim - avoid spending money the wrong way - has been missed.

Stilgoe et.al (2013) discern four dimension of RRI:

- **Anticipation,** instead of traditional risk-management: researchers should ask what-if questions and focus on contingencies, on what is known, what is likely, plausible or possible. Anticipation involves systematic thinking about new opportunities for innovation and the "shaping of agendas for socially-robust risk research" (Stilgoe et.al 2013:3).
- **Reflexivity**: researchers need to be aware of, and even question, their underlying assumptions, values, commitments, the extent of their available knowledge as well as the limits of this knowledge. Most importantly, it should be acknowledged that "a particular framing of an issue may not be universally held" (Stilgoe et.al 2013:4).
- **Inclusion**: it is essential to involve a broad variety of groups, moving beyond a stakeholder approach to also include members of the wider public.
- **Responsiveness**: this involves the capacity to adapt the direction or shape of innovation in accordance with the dynamic change of values among stakeholders and the wider public, also as a result of changing societal circumstances under which an innovation process operates.

While the Action Plan also touches upon the need to look at societal impact even before the R&D phase, there is no clarification what this could mean: "*societal and fundamental rights impact should already be taken into account through societal engagement before and during the R&D phase*" (European Commission, 2012, p.11). Especially in the context of EU-funded research, introducing impact assessment procedures into the R&D process could have far-spread ramifications. Much more reflection, however, is needed, both to better understand which measures are most suitable in each of the phases the R&D process can be segmented into, but also which actors need to be engaged in those phases. For the context of the EU's security research programme, the R&D phase does not necessarily need to be limited to the period after a research project has been positively evaluated and contracted. R&D efforts could also be invested in the pre-submission phase of the project, the formulation of the call for proposals.

It becomes clear from the ASSERT approach that much precision is required to adequately identify and grasp the phase *before* R&D. Elements could be structured around "Negotiating Research", "Defining Research Questions", "Evaluation of Research programmes and projects" (Prainsack and Ostermeier, 2014). Each of these phases requires a specific setup in terms of actors involved.

It seems reasonable that impact assessment mechanisms, implemented at an early stage of technology research and development, or indeed, as the Action Plan states, *before* the

R&D phase, would lead to less costly adaptations (in case results reveal undesired impact) than mechanisms that come into play when most of the research and development decisions are already taken.

One of the most interesting questions probably concerns the fate of a research project that has been identified as having the potential to cause problematic impact (setting aside, for now, methodological issues associated with measuring the societal impact of security research). Again, this would depend on the phase in which the assessment procedure is implemented:

- While in the proposal phase, it may lead to an evaluation which imposes requirements the consortium will have to meet in order to adjust to assessment outcomes;
- Assessing the societal impact of a research project that is already on-going might lead to much greater changes of the project's objectives, scope or methodology.

In conclusion, the Action Plan mentions the Commission's position that

> "[...] the societal and fundamental rights impact should already be taken into account through societal engagement before and during the R&D phase. This would allow addressing societal issues early on in the process" (European Commission, 2012, p.11)

At the same time, the document concedes that "it is extremely difficult to translate societal considerations into technological requirements, which is further complicated by the wide variety of security products on the market" and that "societal issues related to security vary considerably among Member States" (European Commission, 2012, p.11f). It could be argued that the impacts on fundamental rights would require resolution processes based on legal discourses and would differ considerably from wider discourses about the desirability of security solutions (and the formulation of requirements that take into account the needs and views of broader segments of society). For the Action Plan, the "best way forward is to introduce the concept of 'privacy by design' and 'privacy by default' at the design phase" (European Commission, 2012, p.12).

While privacy concerns are of high relevance in the security research and policy discourses, they at the same time fall short of considering other impacts of security measures and technologies and what changes they might facilitate and the desirability of such changes.

Ultimately, the Action Plan remains unclear in what ways "acceptance" of security solutions and technologies is envisaged: are they being accepted because SIA changed the original so completely that an entirely new solution emerged? Or is acceptance envisaged as the result of a public relations effort the aim of which is to dispel possible concerns of potentially affected citizens and members of the public?

5. The ASSERT approach

The ASSERT project[8], working on ways to mainstream societal security in the EU's security research programme, explored different pathways of assessing the societal impact of security research. Its overarching recommendation is to take Societal Impact Assessment seriously. While this may sound blunt and obvious, it has multiple ramifications, as shown in the following chapters. Ultimately, Societal Impact Assessment is about getting better products and services by making better informed design and development choices, building on broad participation and engagement procedures. Those ultimately concerned by security solutions, the citizens, need to be brought closer to security research and the process of target formulation.

While ASSERT did not set out to work towards the goals set out in the Action Plan (better investments and efficiency of investments for the security industry), it can be argued that this would be a side effect of taking SIA seriously. Among other things, such an assessment procedure would have to be endowed with sufficient power and authority in order to have far-reaching consequences for a project. Ultimately, such consequences could include the abandonment of a controversial project altogether.

Based on empirical evidence and building on long-standing assessment traditions beyond *research*[9], the ASSERT-project has developed criteria that delineate promising pathways towards a broader involvement of Impact Assessment mechanisms and approaches in the future. More precisely, these criteria spell out what needs to be done in order for IAs in the context of security research to be successful (and what "success" in this context could mean).

The empirical foundation for these criteria is a series of expert workshops that took place as part of the ASSERT project. There were two main thrusts:

- The first was to scrutinise best practice cases in areas beyond security research, such as biotechnology, and to discuss criteria according to which 'best practices' are most fruitfully and meaningfully established. This included an overview of

[8] http://www.assert-project.eu

[9] Mainly „Social Impact Assessment" as it emerged in the early 1970s, „Constructive Technology Assessment" and „Privacy/ Surveillance Impact Assessment".

the most important conceptual and theoretical tools in the field of Social Impact Assessment (SIA). Part of this process was a reflection on the ways good practices can be transferred from other research fields to the security research domain.

- A second thrust was to identify end user needs, requirements and best practices in social impact assessment (SIA) in security research itself. Part thereof was a discussions that probed the transferability of best practice criteria from wider research areas to the security research field.

In addition to the expert workshop, the ASSERT team drew on literature describing and mapping existing approaches to impact assessment: Social Impact Assessment, Constructive Technology Assessment (CTA) as well as Privacy and Surveillance Impact Assessments (PIA/SuIA) (Prainsack and Ostermeier, 2014). A more detailed discussion of the literature and evolution of these discourses can be found in Prainsack and Ostermeier (2013).

6. Getting impact assessment right: core criteria

Drawing on these sources of existing strands of assessment discourses (SIA, CTA, SuIA, P, PIA) and combining them with expert views collected at the ASSERT workshops, the authors developed a set of core elements which should play a critical in conceiving of any impact assessment process in security research. These core elements, detailed in and elaborated by Prainsack and Ostermeier (2014: pp. 8-13), are presented in the form of questions targeting the planning of an assessment procedure. Their results are used here as a preliminary test case for the EU's Action Plan, by correlating them with the Plan's mention of "checking" or "testing" societal impacts early on in the R&D process:

ASSERT core elements of good SIA practices	Possible ramifications for the EU's Security Industrial Policy
Any SIA should have the potential to change a project's goals and outcomes	• Reframe project objectives • Re-evaluate project outcomes • Redesign envisaged technologies • In extremis: abandon project • "Potential" = Who has the power to intervene in the project? This would differ depending on funding sources, e.g. EU-funded vs. Private funds[10]? What governance structures are appropriate and how "binding" are decisions?

[10] Argueably, private funds invested in technologies not achieving market success are not an externality to EU taxpayers, who in such cases would not bear the risk of inefficient investment.

Take participation seriously	How can industry engage users, societal and research actors and other stakeholders in the most productive manner? Power differentials in determining who has a say in the assessment process have to be tackled: who is likely to benefit from the project's research? How are they likely to benefit? And at whose cost? How can asymmetries be balanced? • SIA can lead to higher acceptance rates of security products or services, but should not be a goal in itself: SIA is about better informed choices, not "acceptance engineering" • In order for a security market based on societal considerations to flourish, the process of identifying societal actors is critical. It should be made clear who identifies stakeholders and actors, and, opening up the debate, what the stakes actually are.
Is the process flexible?	A security industrial policy should develop SIA plans that allow for accommodation of various assessment outcomes during the project's lifecycle
Is the process iterative?	SIA should facilitate iterative processes wherever this is meaningfully possible; however, this can pose a risk for the acceptance of SIA plans in the organisation – are they perceived as a burden or a benefit?
Keep the administrative burden reasonable	• Security industry will inevitably face the challenge of balancing the administrative burden with market efficiency. • SIA plans therefore should aim to balance administrative efforts with the size and scope of the research project. What is reasonable in a huge strategic project may be disproportionate for projects of smaller size. • Can existing SIA plans be used? Can they be scaled up or down? Is there a knowledge base or critical repertory of experiences with such plans? • Can already existing ethical review procedures be tailored to the purpose? • Be very specific about why, at certain points, SIA might create extra work, and how this benefits the overall project
Ensure process transparency	The aims and limitations of the Impact Assessment Plan and its function in a business' innovation process should be made explicit early on, thereby clearly indicating which aspects of societal impact could be considered and which had to be discarded or postponed, e.g. to a retrospective undertaking in the form research evaluation.
Is the prevalent understanding of societal security in a given project clearly defined?	• Where would such a predominant understanding come from? And would it be developed for each project anew, taking into account contextual specific requirements? • Could an authoritative source / definition or catalogue of security practices and societal security contexts be agreed upon and be attributed binding character?
Is societal impact clearly defined?	In an industrial context, there will be a strong need to manage expectations of an assessment procedure, mainly by being clear about what kind of knowledge is produced during its course.
What kind of knowledge is produced in the SIA?	This relates not only to the question what kind of data are being collected and analysed (whether qualitative or quantitative), but also to the nature of this knowledge and its purpose (scientific, political decision making, risk management).

Table 1: Core elements of good practice in assessing the societal impacts of security research in the context of the EU's Action Plan for an innovative and competitive security industry (European Commission, 2012), adapted from Prainsack and Ostermeier (2014).

7. Reconsidering "acceptance" (in light of the principles above)

The calculation is that by providing for impact assessment mechanisms at some point along the R&D phase, public acceptance for security technologies and measures can be secured. This reinforces the above-mentioned statement about organising SIA as a tokenistic exercise, the aim of which would be to go for "acceptance by persuasion" rather than "acceptance by engagement and involvement" (and, eventually, by re-design). The former would not change the outcome of a given research project and rather make every effort to convince the public that no problematic impact is to be expected. The latter would go for acceptance as the result of a research process with the inherent flexibility to change project outcomes when SIA reveals detrimental impacts.

Debates over acceptance and acceptability issues in the EU should also be seen against the background of how the general public in the EU frames science and technology (S&T) and its role in society. According to a 2013 survey, more than half of the respondents are aware that S&T can threaten human rights if applied unethically (Eurobarometer, 2013, p.95). There also seems to be widespread agreement that S&T should not be allowed to make sacrifices to ethical integrity and the inviolability of fundamental rights in order to pursue and justify new discoveries (p.99). The results of the Eurobarometer also make it very clear that the EU is seen as the locus for decision-making on the ethical risks of new technologies:

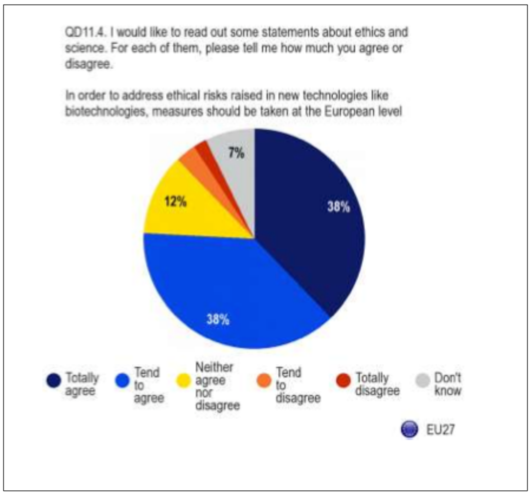


Figure 1: Eurobarometer (2013: p. 108) on Responsible Research and Innovation (RRI), Science and Technology.

Figure 1 shows that an overwhelming majority (76%) of respondents think that measures tackling ethical risks associated with new technologies should be taken at European level. The survey also shows that respondents think that in order for technological innovations to meet the expectations of European citizens, they need to have respect for ethics and human rights. According to the wording, this respect "guarantees" (p.112) meeting citizens' expectations.

Managing risks of research projects or envisaging risks (in terms of impacts) of planned interventions inevitably brings up the question of how risk is framed. Research has shown that the perception of risk and (in-) security do not necessarily operate and develop along linear and rational lines (Slovic, 1987). Rather, diffuse amalgams of socially constructed (and at times also distorted) perceptions, emotions and mental representations of threats and risks prevail, also fed by rumours and hear-say communication. They do so regardless of the outcomes of assessment processes. Public opinion and expert assessment do not walk side by side. This means that while experts in their judgements might be closer to objective facts, the subjective side, or risk perception, is to be taken into account ("the public's fears sometimes don't seem to match the facts", (Ropeik and Slovic, 2003, p.1)). Risk research has also shown that the concept of risk and its perception consists not only of a rational, analytical component, but also of an affective component (ibid.). Among the most common factors that can determine risk perception are dread, sense of control, chosen vs. imposed risks, novelty of the risk, awareness, natural vs. man-made risks (Ropeik and Slovic, 2003, p.2). IA procedures should be aware of the dynamics of risk perception or even, in some cases, the "Social amplification of risk" (Kasperson et al., 1988).

All these aspects about managing risk perceptions should play a stronger role in the implementation of assessment procedures. The practical ramifications of operationalising such an awareness of "risk proliferation" in the context of impact assessment, however, are subject of further research.

8. R&D Phases and Interventions

Another aspect that a determined assessment approach as part of industrial R&D processes would have to consider is that different tools and strategies of SIA apply during the different stages of a research programming cycle. Clearly, SIA mechanisms firing up at different stages of the R&D process will have to focus on different priorities and perform different functions. One of the main and most obvious features of the process is that the nature of the mechanism – over time and from one stage to the next – changes from more prospective to more retrospective: While at the outset of technology development (and, according to the Action Plan (p.11)), "before and during the R&D phase"), the future use and contexts of the security solution are being envisioned[11], the evaluation of research, will, rather, compare outcomes to previously identified and agreed / pre-identified targets. However, an overly normative or prescriptive approach should be avoided here.

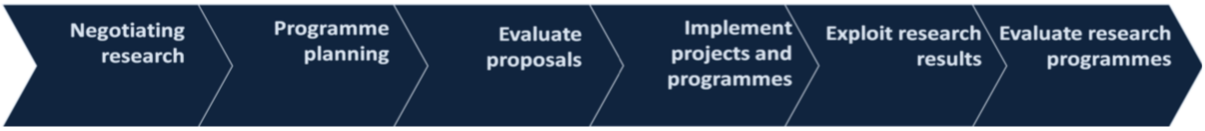
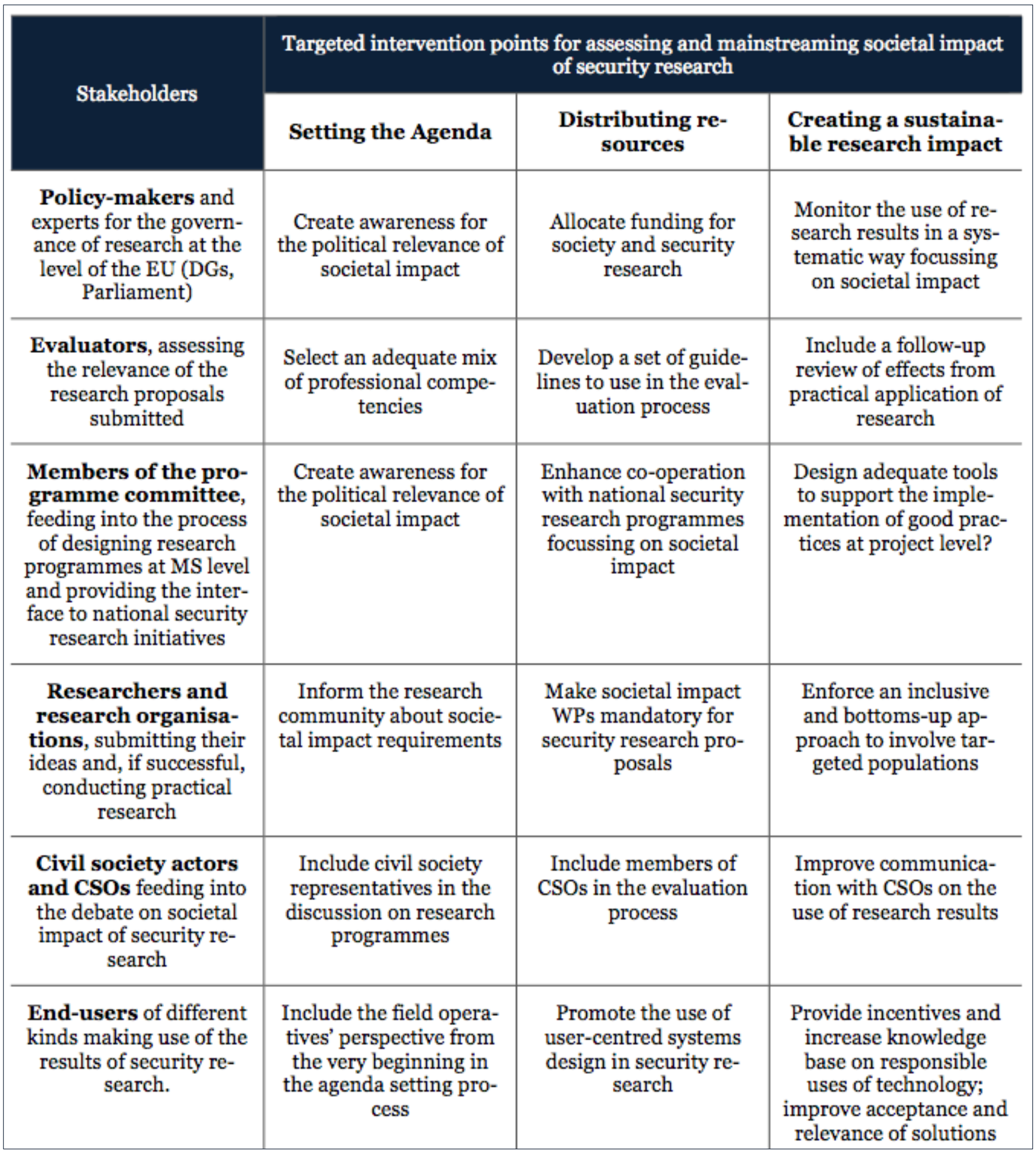


Figure 2: Intervention Points/Phases & Approaches to SIA in security technology R&D . (Ostermeier and Prainsack 2014)

Looking at the research and innovation process as something that can be analytically segmented into subsequent stages also adds value by allowing for a more precise analysis of the actors involved and how to create impact for those different actors. The ASSERT project has developed a matrix that depicts the relevant stakeholders throughout the different phases of the research process and couples them with specific intervention points:

[11] It is this prospective nature of impact assessment procedures which likens the concept to approaches in foresight studies. SIA approaches could (should) also rely on thorough future scenario elaboration and description to set the stage for the assessment of the unintended (negative) consequences of technology development.



Stakeholders	Targeted intervention points for assessing and mainstreaming societal impact of security research		
	Setting the Agenda	**Distributing resources**	**Creating a sustainable research impact**
Policy-makers and experts for the governance of research at the level of the EU (DGs, Parliament)	Create awareness for the political relevance of societal impact	Allocate funding for society and security research	Monitor the use of research results in a systematic way focussing on societal impact
Evaluators, assessing the relevance of the research proposals submitted	Select an adequate mix of professional competencies	Develop a set of guidelines to use in the evaluation process	Include a follow-up review of effects from practical application of research
Members of the programme committee, feeding into the process of designing research programmes at MS level and providing the interface to national security research initiatives	Create awareness for the political relevance of societal impact	Enhance co-operation with national security research programmes focussing on societal impact	Design adequate tools to support the implementation of good practices at project level?
Researchers and research organisations, submitting their ideas and, if successful, conducting practical research	Inform the research community about societal impact requirements	Make societal impact WPs mandatory for security research proposals	Enforce an inclusive and bottoms-up approach to involve targeted populations
Civil society actors and CSOs feeding into the debate on societal impact of security research	Include civil society representatives in the discussion on research programmes	Include members of CSOs in the evaluation process	Improve communication with CSOs on the use of research results
End-users of different kinds making use of the results of security research.	Include the field operatives' perspective from the very beginning in the agenda setting process	Promote the use of user-centred systems design in security research	Provide incentives and increase knowledge base on responsible uses of technology; improve acceptance and relevance of solutions

Table 2: Stakeholders and intervention points across the phases of the research and innovation process (taken from the ASSERT-project's Description of Work)

Inevitably, this brings up the question of scale: Looking at ways to (re-negotiate) an entire research funding programme is an endeavour very different from looking for ways of integrating societal security concerns in a project's proposal phase or in a project's evaluation phase (also, different types of knowledge are required, especially with regard to project evaluators which would require specific training in order to understand whether a project has sufficiently taken into account societal impacts).

9. Conclusions

The Commission's Action Plan aims to reinforce the societal dimension of security research and technology. It does so for a very clear motivation, which is to improve market conditions for industry and heighten investment efficiencies. The role foreseen for impact assessment is to make sure that newly developed technology hitting the market is met by public acceptance (and can thus be sold). The relationship between SIA and acceptance is not clearly spelt out. Impact assessment appears as a marketing activity, focusing on risk communication at best. The process of negotiating research objectives and priorities, however, should not only be opened up, but also be enshrined in a mechanism with the power to reframe or even, in extreme cases, abort a publicly funded research project. One of the difficulties of the Action Plan appears to be its underlying assumption that the testing mechanism per se will guarantee a security technology can be sold. In this lies the danger of perceiving impact assessment efforts as a measure to promote a project's legitimacy. Rather, a situation should be contemplated in which the testing mechanism discards a research project's objectives or entirely. And this is precisely what will most likely ignite controversy: how should we endow an assessment process with sufficient power that it will be able to transform a project in such a fundamental way?

References

ESRIF (2009): Final Report of the European Security Research and Innovation Forum. [online]. Available from: http://ec.europa.eu/enterprise/policies/security/files/esrif_final_report_en.pdf [3 June 2014].

Eurobarometer (2013): Resonsible Research and Innovation (RRI), Science and Technology (Special Eurobarometer 401) [online]. Available from: http://ec.europa.eu/public_opinion/archives/ebs/ebs_401_en.pdf [3 June 2014].

European Commission (2013): Options for strengthening Resonsible Research and Innovation. Report of the Expert Group on the State of Art in Europe on Responsible Research and Innovation [online]. Available from: http://ec.europa.eu/research/science-society/document_library/pdf_06/options-for-strengthening_en.pdf [3 June 2014].

European Commission (2012): Security Industrial Policy Action Plan for an innovative and competitive Security Industry (COM(2012) 417 final) [online]. Available from: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0417:FIN:EN:PDF [3 June 2014].

Kasperson, R. E. et al. (1988) The Social Amplification of Risk: A Conceptual Framework. Risk Analysis. 8 (2), 177–187.

Prainsack, B. & Ostermeier, L. (2014): Report on good practices of the exploration and assessment of the societal impact of research. ASSERT Project Deliverable 1.3 [online]. Available from: http://assert-project.eu/wp-content/uploads/2014/03/ASSERT_D1.3_fin.pdf [3 June 2014].

Prainsack, B. & Ostermeier, L. (2013): Report on methodologies relevant to the assessment of societal impacts of security research. ASSERT Project Deliverable 1.2 [online]. Available from: http://assert-project.eu/wp-content/uploads/2013/04/ASSERT_D1.2_KCL_final.pdf [3 June 2014].

Ropeik, D. & Slovic, P. (2003): Risk Communication: A neglected Tool in protecting Human Health. Risk in Perspective 11, (2) [online]. Available from: http://www.hcra.harvard.edu/rip/risk_in_persp_June2003.pdf [3 June 2014].

Slovic, P. (1987): Perception of Risk. Science 236 (4799), 280–285 [online]. Available from: http://socsci2.ucsd.edu/~aronatas/project/academic/risk%20slovic.pdf [3 June 2014].

Stilgoe, J. et al. (2013) Developing a framework for responsible innovation. Research Policy. [Online] 42 (9), 1568–1580. [online]. Available from: http://linkinghub.elsevier.com/retrieve/pii/S0048733313000930 [12 August 2014]. DOI: 10.1016/j.respol.2013.05.008.