Science and Public Policy **42** (2015) pp. 339–354
Advance Access published on 25 August 2014
doi:10.1093/scipol/scu046

The state of the art in societal impact assessment for security research

Kush Wadhwa, David Barnard-Wills* and David Wright

Trilateral Research, Crown House, Hammersmith Road, London WH14 8TH, UK;
**Corresponding author. Email: david.barnard-wills@trilateralresearch.com.*

This paper sets out a structured methodology for conducting a societal impact assessment (SIA) of security research and security measure implementation. It first provides an overview of the need for and role of SIA, then presents an account of the existing impact assessment methodologies that have influenced this guide. The paper then describes the core methodology based upon an iterative approach to six key sectors of impact, then provides analytical questions for use in this process, before setting out a step-by-step process guideline. This guideline includes guidance on identifying stakeholders and incorporating best practice in impact assessment. Guidance on the content of an SIA report is then provided. The paper concludes with recommendations as how to best embed such a methodology within the broader security research process. The methodology has particular relevance for security research conducted within the EU.

Keywords: security; impact assessment; societal impact; research; consultation.

1. Introduction

This paper sets out a structured methodology for conducting a societal impact assessment (SIA) of security research and security measure implementation. The paper first provides an overview of the need for and role of SIA, then presents an account of the existing impact assessment methodologies that have influenced this guide. Section 2 describes the core methodology based upon an iterative approach to six key sectors of impact, then provides analytical questions for use in this process, before setting out a step-by-step process guideline, including guidance on identifying stakeholders and incorporating best practice in impact assessment. Section 3 provides guidance on the content of a SIA report. The paper concludes with recommendations as to how best embed such a methodology within the broader security research process. The methodology has particular relevance for security research within the EU, however, as the approach is based upon principles and methodology rather than legal compliance, it therefore has a wider potential applicability.

1.1 Societal impacts of security research

Security research and innovative application of security technologies is a complex and heterogeneous field that pulls together various academic disciplines and different types of organisation. Several features characterise the field of security research. These features include ethical and social issues that have been identified by different research fields.

Security itself is socially and institutionally valued, attracting significant funding streams and market attention. The security industry is regarded as an important economic sector for Europe (McCarthy 2012, European Security Research Advisory Board). Security has a particular institutionalisation within policy-making communities (Chilton 1996: 23). Security research programmes, such as the EU's Secure Societies effort (European Commission (2013b), therefore take place within these social, economic and political contexts, their ends goals being not just security, but also industrial development.

Identifying some feature of the world as a security issue is to grant it a particular privileged political status and to start to frame the issue in a specific way: deserving political and social responses and identifying it as the responsibility of certain political actors (Buzan et al. 1998). This framing of what counts as a security risk is known as securitization and has been the subject of considerable research within international relations security studies (Buzan and Hansen 2009, Neocleous 2007). Similarly, security practices, including research and innovation, can contribute to the normalisation

of security (Nissenbaum 2009: 161), with security becoming an organising principle across many areas of social life, sometimes to the detriment of other values or principles, such as: privacy, transparency, freedom of speech or the democratic process. Security impacts can be powerful, and are frequently distributed unevenly across society (e.g. border security measures may be intended to increase national security, but can increase insecurity for asylum seekers and immigrants). Some groups are particularly vulnerable to the negative impacts of security research and implementation and are often excluded from decision-making processes. These groups can suffer from cumulative disadvantage which, in turn, can have negative implications for social cohesion (Lianos 2000). Security processes often have the potential to negatively impact citizens' fundamental rights.

Security (and security research) is part of the political process. However, societies often experience periods of delay between the societal impacts of security policy and intervention, social awareness of these impacts, their examination in the democratic process and responses to them from law and regulation. During this lag, security practices and technologies can become entrenched in areas of social life making it difficult to dislodge them. A related problem is function creep, where security technologies installed for one purpose are used for secondary, initially unintended or unstated uses. Misalignment and disjunction between agencies and actors with responsibility for promoting security technology, and those with responsibility for assessing, controlling and in some cases limiting and preventing negative impacts, can also exacerbate these situations (Rip and Schot 1997).

Security research, especially in the fields of crime prevention and national security, often has less transparency than in areas where national interests are not seen as affected in such an immediate way, and governmental bodies are less centrally involved. There is limited public access to knowledge about the research. This often serves to exclude stakeholders, while at the same time limiting the acceptability of security measures, causing them to be viewed with suspicion.

It is important for the people and institutions involved in both security research and the innovative application of security technologies to consider the wide range of possible societal impacts of these activities, as a response to the above political and social issues, and as part of maximising the positive social benefits of security research whilst minimising the negative effects. SIA therefore has a critical role in the security research and implementation process.

SIA is the process of understanding, managing and responding to the societal impacts that arise from security research and the application of innovative security measures. The use of the term societal (rather than social) connotes the inclusion of anything affecting human, natural or artefactual systems, rather than just those effects that impact upon humans and their interactions. It also allows us to distinguish the process from social impact assessment, as discussed below.

From a positive perspective, SIAs can also provide a better understanding of the productive and socially desirable impacts that arise from security research, including how best to maximise these contributions. Conducting impact assessment exercises as part of security research and innovation contributes towards the evidence base for these activities. SIA can contribute towards understanding the societal impact of larger scale research funding frameworks and policies, including their contribution towards policy objectives (e.g., the partial goal of EU security research funding in boosting the competitiveness of the EU security industry).

Security research and innovation are, by definition, intended to produce, encourage or support security as societal impact. An inclusive definition of security includes those practices and technologies aimed at strengthening social bonds and social resilience using social policy tools as well as just preventive measures against particular threats. This understanding of security aligns with the concept of human security (United Nations 2012). Rather than conceptualising security as an outcome of using security technologies, security is conceptualised here as one of the societal impacts of security measures. Although security research and the implementation of security measures have internal differences, this paper discusses them together, as they are both amenable to the assessment approach set out here.

1.2 Influences on SIA

SIA for security research has not emerged in a vacuum. SIA approaches draw upon a range of previously established methodologies and practices, both in security research and related areas. These influences include: constructive technology assessment (CTA), privacy impact assessment (PIA) and recent developments in surveillance impact assessment (SuIA), SIA and the impact assessment activities of the European Commission. There is some limited influence from the responsible research and innovation debate and from research ethics, although this is primarily concerned with the way that research is conducted, rather than concerns about the goals and subjects of the research (McCarthy 2012: 10).

CTA is defined by Rip and Schot (1997: 251) as an approach that:

> ... shifts the focus away from assessing impacts of new technologies to broadening design, development, and implementation processes ...

the aim of which is to contribute:

> ... better technology to a better society.

By anticipating impacts, involving users and stakeholder communities in the design process in an interactive manner and by harnessing social learning, it is possible to avoid the

human costs associated with trial-and-error social responses to new technologies. Social aspects of technologies are explicitly included as design criteria (Rip and Schot 1997: 251). CTA claims no inherent normative agenda, rather focusing upon expanding the reflexivity of the design process, however, it serves to close conflicts and increase acceptance. Tools and procedures of CTA include: understanding the innovation journey, identifying points of intervention at different phases of a project, anticipating the outcome of a research process, reflexivity exercises, stakeholder workshops, technology forcing (Genus 2006: 19) and strategic niche alignment (Schot & Geels 2008).

PIA is a methodology for assessing the impacts on privacy of a project, policy, programme, service, product or other initiative that involves the processing of personal information and in consultation with stakeholders for taking remedial action as necessary in order to avoid or minimise negative impacts (Wright and de Hert 2012: 5). SuIA is an expansion of PIA that takes into account a wider range of issues, impacts and stakeholders across the surveillance system (Wright and Raab 2012). The aims of PIA and SuIA are: better privacy protection, increased transparency of personal information processing technologies and increased accountability (and for SuIA mitigation of the risks of surveillance systems). It is also intended to engage stakeholders and affect the direction of a project from its earliest stages. PIA has been adopted across several countries (Wright 2013).

Potentially the broadest of the influential approaches, SIA as understood by Vanclay (2003:2) is a participatory process for the analysis, monitoring and management of the intended and unintended, positive and negative consequences of planned interventions. The goal is a more sustainable and equitable physical and human environment, and key methods include: increasing awareness of potential unintended consequences, through the exploration of the likely impacts of a research project on people's lives, cultures, communities, political systems, environment, health and wellbeing, personal and property rights, fears and aspirations.

As part of the legislative process, the European Commission undertakes impact assessments of policies, legislation, trade agreements and other measures. This includes publishing roadmaps and economic, social and environmental impact assessments of planned initiatives prior to EU action. Post-intervention, this is followed by evaluation of the performance of initiatives and by subjecting them to regulatory fitness and performance assessment. The Commission seeks public consultation throughout the process (European Commission 2014).[1]

The three theoretical approaches share reflexivity as core principles, and all four approaches have a strong focus on participation. Similarly, the approaches all share the perspective that impact assessments should be initiated at the earliest possible stages of a project or intervention, and conducted as an ongoing activity. SIA contributes the need for an awareness of societal dimensions and how they impact the security R&D process. It highlights stakeholder dissatisfaction with the reports of existing social impact processes, especially post-impact studies, and the importance of a social impact assessment as a tool and investment in risk management (Vanclay and Esteves 2011: 11). CTA recommends researchers exercise critical reflexivity and emphasises the prominent role of societal issues in research consortia (Rip and van Lente 2013). In their attempt to combine CTA and SIA, Russell et al. (2010) in what they call a 'technology assessment in social context', draw upon social science approaches to increase the extent to which social issues are included in a technology assessment. Their approach also highlighted the importance of stakeholders, and expressed the explicit aim of:

> ...facilitating interactions between technology developers, decision makers and users. (Russell et al. 2010: 111)

The European Commission's impact assessment process—which currently is applicable only to policies developed by EU institutions—demonstrates the value of publishing impact assessments and building a common methodology within a sector. SuIAs already include privacy and ethical impact assessments and are therefore a suitable model for rigorous impact assessment. Table 1 shows the influences from existing approaches that have contributed to the SIA approach set out in this paper.

As a broad category of practice, SIA therefore includes the other approaches (see Fig. 1). The existing approaches are all forms of societal impact. In this paper we draw upon these existing best practices to present a composite approach that is applicable to security research.

2. Step-by-step guide for SIA in security research

The objective of the SIA process is to increase the reflexivity of the process and of decision-making, not to prescript or pre-define the results of an assessment process. Reflexivity in this context is the ability of researchers to take stock of their role in the research process, and subject their research activity to the same level of critical scrutiny as the rest of their 'data' (Mason 1996). Reflexivity is a process of critical reflection both on the kind of knowledge generated from research and on how that knowledge is generated (Guillemin and Gillam 2004). Reflexivity and an openness to alternatives is crucial to act upon the 'irritation' that SIA is capable of creating by ensuring that those results that challenge the core assumptions of the planned project, technology or policy can also have an impact on the planning process. One cannot assume a simplified binary process in which security technologies are invented, and then go on to have implications and

Table 1. Combination of elements across impact assessment

Elements of societal impact assessment	Influences from existing approaches			
	Social impact assessment	Privacy impact assessment	Constructive technology assessment	European impact assessment
Including all human, natural and artifactual systems	Human interactions/social dimensions		Inclusion of social science in technology assessment	
Critical reflexivity of assessment	Reflexivity towards societal dimensions		Critical reflexivity	
Stakeholder involvement	Stakeholder involvement	Stakeholder involvement	Stakeholder involvement	Stakeholder involvement
Publishing				Publishing
Common methodology				Common methodology

impacts (Rip and Schot 2002). Innovation studies have established the observation that innovation frequently does not occur in a linear process but in a complex and uncertain process of trial, error and unintended developments (Braun-Thürmann 2005). As with PIA (Wright 2013), one size does not fit all with regard to SIA, and this methodology should be adaptable to the specific needs and contexts of a given research project or innovation. Using a shared framework and accepted common approach increases the transferability across domains of the assessment, and is likely to increase external confidence in the process. The offered approach is rigorous and detailed. This is because a security research project is often operating in relatively unknown or conjectured terrain. The additional information produced for such a project by a detailed impact assessment supports better understanding of the security intervention being researched.

2.1 Methodology

The core of the methodology proposed is based upon analysis driven by interaction with the stakeholders and posing a series of questions that enable the discovery of varying views on impacts. This enquiry is divided into six different aspects of societal impacts as shown in Fig. 2, and the enquiry is completed in an approach commonly used in curriculum design[2] (moving from basic questions to increasingly more complex ones as more is learnt, cycling or spiralling back through the same topics multiple times).

The various aspects of societal impact that are evaluated include those suggested by Vanclay (2003: 7) (attributed in part to ideas developed by Armour), which have been combined here into six main groups:[3]

- *way of life, fears and aspirations* (how people live and interact with each other on a daily basis, their perceptions about their safety and that of their communities, and their aspirations for future, including the future of their children)
- *culture and community* (people's shared beliefs, customs, values and languages, the cohesion, stability and character of their communities)
- *political systems* (participation in the decisions and processes that affect people's lives, the nature and functioning of democratic processes, and the resources available to support people's involvement in these)
- *environment* (access to and quality of air, water, and other natural resources, the level of exposure to pollutants and harmful substances, adequacy of sanitation)
- *health and wellbeing* (physical and mental wellbeing, not just an absence of infirmity)
- *personal and property rights* (economic effects, civil rights and liberties, personal disadvantage)

The assessor should start the SIA evaluation process by looking at any one of the above aspects in three different dimensions:

- First, examine whether the security research project meets the needs of society.
- Iterating a second time through the same six aspects, review the potential externalities or costs to society, enumerating risks and identifying ways to mitigate them.
- Finally, pass through the six societal impact aspects a third time to identify potential benefits to society.

With each re-evaluation of the six aspects, the assessor and stakeholders have the opportunity to rethink answers to previous questions based upon answers across each of the earlier assessments, providing an opportunity to go back and rethink impacts where new information has been brought to light or where new ideas have emerged.

The following set of questions (see Table 2) provides a basis for examining the social needs, potential costs and risks, and potential benefits of security research. The questions are based upon the societal impact checklist for R&D developed by the Societal Impact Expert Working Group in their report to the European Commission's Directorate-General for Enterprise and Industry (McCarthy 2012).

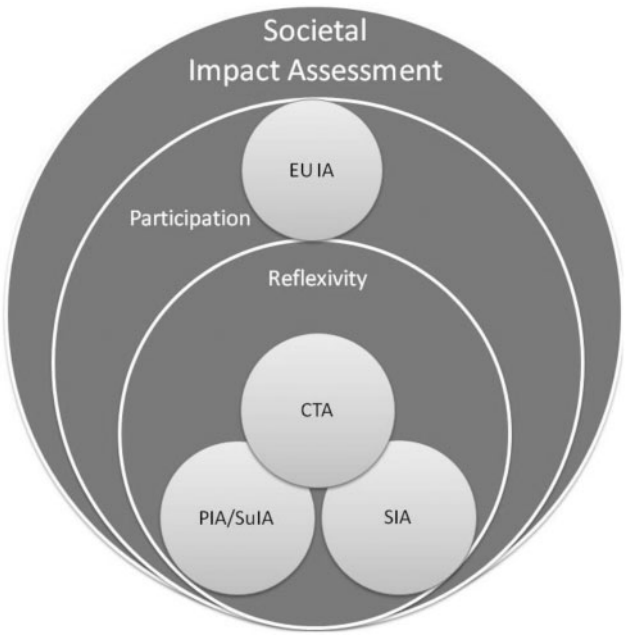

Figure 1. SIA methodologies.

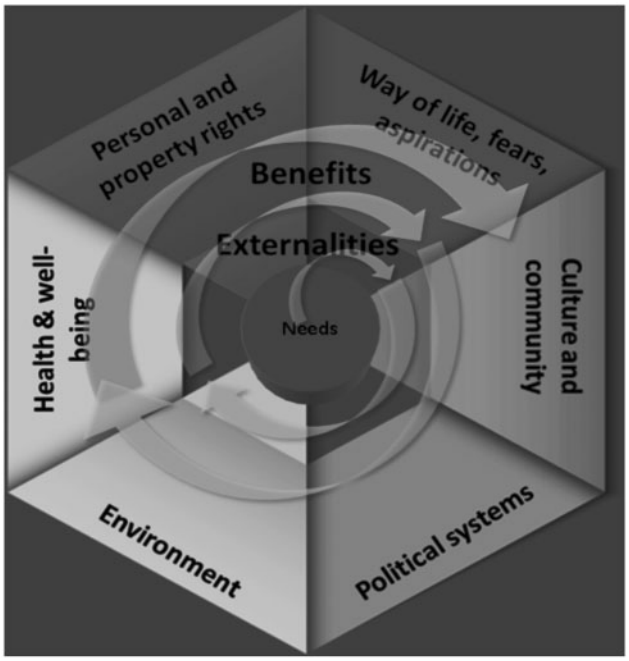

Figure 2. Methodology.

2.2 Process

To effectively employ this evaluation methodology, it should be put in the context of the following 15-step process (see Table 3). This process is based upon PIA methods, and shares common features with the EU impact assessment procedure (European Commission 2013a). As the project progresses, there is a shift from foresight, to management, to evaluation. Guidance for each individual step in the process is provided below.

2.2.1 Preparation and planning. This approach acknowledges that for many types of security research, there is a need to conduct SIAs during the research planning or proposal stage. At this stage, there may be minimal resources available to support extensive societal impact efforts, including in-depth consultation. Structured consideration of societal impact at this stage can improve the quality of the research design being proposed or considered, and is crucial to ensure that negative societal impacts are not locked into the research design.

2.2.1.1 Identify the SIA team and set the team's terms of reference, resources and time frame. The research project manager should be responsible for the conduct of a SIA, but she may need some additional expertise, perhaps from outside her organisation. Depending on the estimated scale of the SIA, the project manager or the designated societal impact assessor may need to form a team to undertake the SIA. The team could bring together expertise from information security experts, lawyers, operations managers, ethicists, public relations experts etc. As the SIA progresses, the assessor may find that she needs still other expertise. The benefits of a dedicated manager and interdisciplinary team, which ideally includes some social science expertise, is supported by existing methodologies of social impact assessment (Kemp 2011: 30). Eurobarometer research suggests that the European public is most receptive to accounts of research that come from researchers themselves (European Commission 2013c).

The project manager and/or the organisation's senior management should decide on the terms of reference for the SIA team, its budget and its time frame. The assessor may come under considerable pressure to complete the SIA quickly so as not to delay the project, but she may need to resist compromising the integrity and adequacy of her SIA mission and may need to ensure she has the full support of the organisation's CEO and/or its management board. The terms of reference should make clear that the SIA is a process, and that the process will need to continue beyond preparation of the SIA report. If the assessor's work or that of an external consultant comes to an end with publication of the report, the project manager and/or the organisation's CEO and/or management board should decide how implementation of recommendations will be monitored and who will be responsible for the monitoring and what factors will determine whether the SIA report needs to be updated.

For research projects, it may be appropriate to dedicate a work package or stream of activity to the societal impact role. If this is done, it is important to ensure that this work package is integrated with the other elements of the project, perhaps through shared personnel or making later elements of the work dependent upon stages of the SIA report.[4]

Table 2. Assessment questions

Meets needs of society?	1. Which documented societal security need(s) does the proposed research address (e.g. life, liberty, health, employment, property, environment, values)? 2. How will the research output meet these needs? How will this be demonstrated? How will the level of societal acceptance be assessed? 3. Is the research project aware of challenges to these needs? 4. Does addressing the documented societal needs through the proposed research require any trade-offs with other documented societal needs? How is this trade-off decided? Is this trade-off still valid if the research is less effective than anticipated? 5. What threats to society does the research address (e.g. crime, terrorism, pandemic, natural and man-made disasters)? 6.How is the proposed research appropriate to address these threats? 7. What other measures could be adopted to address these threats?
Ensuring security research does not have negative impacts on society	8. How could the research have a negative impact on human dignity? 9. . . . on the right to life? 10. . . . on equality before the law? 11. . . . on freedom of thought? 12. . . . on freedom of opinion and information? 13. . . . on privacy? 14. . . . on protection of the family? 15. . . . on freedom of movement? 16. . . . on rights of ownership? 17. . . . on freedom of assembly? 18. . . . on freedom to choose an occupation? 19. . . . on working conditions? 20. . . . on collective social rights? 21. . . . on social welfare? 22. . . . on rights to an education? 23. . . . on the principle of democracy? 24. . . . on rights of access to information? 25. . . . on rights of access to the courts? 26. . . . on access to public space? 27. If implemented, how could the research have a negative impact on this aspect (culture and community, way of life etc.)? 28. How could the research impact disproportionately upon specific groups or unduly discriminate against them? How could the research increase discrimination?Could the research have impacts upon vulnerable groups (including, but not limited to: women, the elderly, disabled people, children and young adults, homeless people, economically disadvantaged people and people in precarious situations, immigrants or non-citizens, and lesbian, gay, bisexual, transgender or queer identifying people?
Ensuring security research benefits society	29. What segment(s) of society will benefit from increased security as a result of the proposed research? 30. How will they benefit? 31. Are additional measures required to achieve this benefit? 32. Are additional measures possible to extend these benefits to other segments of society? 33. In what contexts might this benefit be lacking or not be delivered by the research project? 34. How will society as a whole benefit from the proposed research? 35. Are there other European societal values that are enhanced by the proposed research, e.g. public accountability and transparency; strengthened community engagement, human dignity; good governance; social and territorial cohesion; sustainable development?

2.2.1.2 Prepare the SIA plan. The assessor should prepare a plan for conducting the SIA. She can prepare the SIA plan using this SIA process document, but may need to tailor it to the exigencies of the project to be assessed. The plan should spell out the objectives of the SIA, what is to be done to complete the SIA, who on the SIA team will do what, the SIA schedule and, especially, how the consultation will be carried out. An important part of the plan should address consultation. It should specify why it is important to consult across each of the six societal impact areas, who will be consulted and how they will be consulted (e.g. via public opinion survey, workshops, focus groups, public hearings, online experience, specialist consultation tools).

The SIA should also include if and how societal impact will be included in any post-research evaluation activity.

2.2.1.3 Determine the budget for the SIA. Once the project manager and/or assessor have prepared an SIA plan, they can estimate the costs of undertaking the SIA and seek the budgetary and human resources necessary from the organisation's senior management. Unfortunately, the assessor may be constrained in what she can do in the SIA by the budget allocated by the organisation. If the assessor is unable to do an adequate SIA, she should note this in her SIA report. The assessor may need to revise her SIA plan based on the budget available.

In general, the budget for performing an effective SIA will depend upon a number of factors, including: first, the stage at which an SIA is being performed; and second, the scale, scope, and overall complexity of the project. For example, if an SIA is being performed at the inception of the project, while there remains adequate opportunity to

Table 3. Steps in the SIA process

Preparation and planning	1. Identify the SIA team and set the team's terms of reference, resources and time frame
	2. Prepare the SIA plan
	3. Determine the budget for the SIA
	4. Describe the project to be assessed
	5. Identify stakeholders
Consultation and analysis	6. Conduct the spiral assessment of the six core areas of societal impact to identify impacts associated with needs, externalities/costs, and benefits
	7. Consult with stakeholders
	8. Determine whether the project complies with legislation. Assess whether the security research has the potential to generate results that require new legislation to address potential gaps
	9. Identify risks and possible solutions
	10. Formulate recommendations
Reporting and responding	11. Prepare and publish the report, e.g. on the organisation's website and/or in a suitable repository
	12. Implement the recommendations
	13. Ensure a third-party review and/or audit of the SIA
	14. Update the SIA if there are changes in the project
	15. Refer to the SIA in any post-project evaluation

effect change, it may be more cost-effective than if the SIA is performed after a great deal of research, design, and development has been completed.

As a matter of practical estimation, it can be expected that the SIA will require budget for the salary of a senior-level consultant and a junior-level consultant for approximately one person-month, presuming that the consultants are experienced in performing SIAs and come to the task already armed with procedures and templates to perform it. If so equipped, they will use some of their time to understand the project and subsequently survey or interview key stakeholders before completing their analysis. If this is the first time an organisation has undertaken an SIA, they will need to take an extra two or three months to develop their process before beginning the work of the SIA itself. Experienced consulting companies will have already completed this work, and of course, there will likely be additional costs of addressing the outcomes of the SIA (potentially greater if the SIA is performed later in the R&D cycle). Additional indirect costs may be incurred by other project partners as they inform and collaborate with the SIA team.

2.2.1.4 Describe the project to be assessed. The assessor should describe the project or technology or service to be assessed. As the development of the project or technology or service may still be at an early stage, there may not yet be that much known about the project. The assessor can update the description as more becomes known. The description can be used in at least two ways: it can be included in the SIA report and it can be used as a briefing paper for consulting stakeholders. The description of the project should provide some contextual information (why is the project being undertaken, how is it funded, who are the project members and participants, who are the intended audiences for the findings of the research, how it relates to other ongoing security research activity conducted by the project members). The project description should state who is responsible for the project. It should indicate important milestones and, especially, when decisions are to be taken that could affect the project's design.

2.2.1.5 Identify stakeholders. A critical component of SIA is the participative inclusion of stakeholders in the assessment of the security research project or security measure application. The assessor should identify stakeholders, that is, those who are or might be interested in or affected by the project, technology, service or other initiative. The stakeholders could include people who are internal as well as external to the organisation. Involving a variety of stakeholders provides an opportunity for any potential risks to be highlighted and eventually managed. Given the potential breadth of societal impact across different categories of impact, the way that 'stakeholders' is understood should be broad and inclusive.

Kemp (2011) provides a list of parties who could potentially be affected by a planned project or policy and should thus be engaged within the context of SIA. Building upon this list, and customising it for the security research process provides the following summary:

- personnel or managers with carriage of the social agenda within project proponent organisations
- researchers, designers, engineers, developers, potential suppliers, security experts and others who will carry out the research activity
- assessors who are commissioned to undertake or facilitate the SIA process, either internally or from outside of the organisational structure of the project proponent
- project-affected peoples, up to and including representatives of the general public
- regulators

- civil society organisations, including civil rights advocates
- the media
- academics
- businesses

The assessor should identify these different categories and then identify specific individuals from within each category, preferably as representative as possible. The stakeholders of a project, and particular people who might be affected by the project, will be dependent upon the context of the project and the way in which it is conducted. This means that the above list cannot be inclusive and the project assessor must make efforts to identify other stakeholders as appropriate. Social relations are complex, and stakeholders, especially those affected by unintended consequences, may not be apparent to the SIA team. The SIA process should therefore include opportunities for individuals, groups and organisations to self-identify as stakeholders and request participation in the assessment activity. Some stakeholders may only become apparent as the SIA progresses. If necessary or useful, they too should be brought into the consultation process. The range and number of stakeholders to be consulted should be a function of the likely societal impact as identified in early stages of the spiral methodology, including the number of people who could be affected. Thus, the number of stakeholders to be consulted could be relatively limited if the project or service is also expected to be small, for example, the project or service might only involve employees of a small or medium-size enterprise. The proper involvement of stakeholders may require additions to the SIA team, either to encourage participation by stakeholders, or to bring in key stakeholders, who may be most affected by the project into the SIA team directly.

2.2.2 Consultation and analysis. The four stages in this section involve the analysis of societal impacts using an iterative process based upon the methodology, and in concert with identified stakeholders, that looks at each of six aspects of societal impacts as described above.

2.2.2.1 Consult with stakeholders. The project manager and/or societal impact assessor should enter a dialogue with as many stakeholders as is appropriate or meaningfully possible (taking into account the available budget). There are many reasons for doing so, not least of which is that they may identify some societal risks not considered by the project manager or assessor. By consulting stakeholders, the project manager may forestall or avoid criticism that they were not consulted. If something does go wrong downstream—when the project or technology or service is deployed—an adequate consultation at an early stage may help the organisation avoid or minimise liability. Furthermore, consulting stakeholders may provide a sort of 'beta test' of the project or service or technology. Consulted stakeholders are less likely to criticise a project than those who were not consulted. The earlier a consultation process is entered into, the more benefits an organisation can expect to draw from it as any learning produced can be integrated into the project more rapidly, and additional information may help to avoid unanticipated problems in the project.

There are several different ways of consulting stakeholders and the assessor should consider which will be most appropriate in the circumstances. The assessor or other members of the SIA team could interview stakeholders directly. They could convene workshops of experts or stakeholder representatives. They could hold focus groups of ordinary consumer-citizens. They could conduct surveys by telephone or email or face to face. They could post the project description on the organisation's website and invite comments. They could hold public hearings where they describe the project and invite comments from the audience or from experts and then invite comments after the experts have spoken. They could prepare stories or adverts in the media and invite comments from readers. They could conduct a Delphi survey of experts, to query them on potential societal risks now and in the future.[5] There are current EU-funded research projects which are working to produce structured methods for consultation in security research.[6]

SIA has attracted a range of cautionary comments in relation to community participation: that participation can become a tokenistic exercise, can be inconsistent, often does not involve enough participation in actual decision-making, being reduced to a form of consultation (Bishop and Davies 2002; Müth 2003; O'Faircheallaigh 2010; Peterman 2004). Moreover, community participation is sometimes used as a seeming quick fix for problems, without addressing the root of the issue (which often lies in unequal power distributions that are deeply engrained in polities, and sometimes in the very institutions of the community whose participation is sought). As a result, community participation sometimes takes the form of a tokenistic exercise; once 'affected communities'—or their leaders—have been heard, the respective box can be ticked off, and afterwards the rule of previous power relations resumes (Peterman 2004). To avoid this, the participation of stakeholders in an SIA exercise should be dialogic and a partnership, and go beyond simply writing down what stakeholders have to say. Stakeholders should have access to the researchers and ideally be able to exercise some influence over the direction of the project.

2.2.2.2 Compliance with legislation. A SIA for security research is more than a compliance check. Nevertheless, the assessor or her legal experts should ensure that the project complies with any legislative or regulatory requirements. These may be high-level laws relevant across

Table 4. Potentially applicable legislation at the EU level (source: authors)

Way of life, fears and aspirations	Charter of Fundamental Rights of the European Union; European Convention on human rights; Council Directive 2000/78/EC of 27 November 2000 establishing a general framework for equal treatment in employment and occupation; Directive 2004/38/EC on the right to move and freely reside; Gender recast Directive 2006/54/EC; Employment equality Directive 2000/78/EC/
Culture and community	Charter of Fundamental Rights of the European Union; Council of the European Union, Directive 2000/43/EC of 29 June 2000 implementing the principle of equal treatment between persons irrespective of the racial or ethnic origin; Racial Equality Directive 2000/43/EC
Political systems	Charter of Fundamental Rights of the European Union; European Convention on Human Rights
Environment	Directive 2008/1/EC of the European Parliament and the Council of 15 January 2008 concerning integrated pollution prevention and control: Directive 2011/92/EU of the European Parliament and the Council of 13 December 2011 on the assessment of the effects of certain public and private projects on the environment
Health and wellbeing	National legislation for health; Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare; Council Directive of 12 June 1989 on the introduction of measures to encourage improvements in the safety and health of workers at work (89/391/EEC)
Personal and property rights	Charter of Fundamental Rights of the European Union; Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data; Directive 2002/58/EC of the European Parliament and the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector; Employment Equality Directive 2000/78/EC; Gender goods and services Directive 2004/38/EC; Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters

contexts, such as (at the European level) the European Convention on human rights (<http://www.echr.coe.int/Documents/Convention_ENG.pdf> accessed 7 Jul 2014) and the EU Charter of Fundamental Rights (European Parliament et al. 2010) as well as more specific laws, regulations, codes and guidelines applicable to the specific context and aims of the project being assessed. Research projects attracting institutional support will also have to comply with relevant standards and criteria selected by funding or sponsoring institutions. Individual institutions will likely have their own guidance on this, which should be identified here. The exercise of producing the SIA report will likely assist in compliance with these requirements.

Table 4 presents some legislation at the EU level that may be applicable to security research projects.

2.2.2.3 Identify societal impacts and possible solutions. The assessor and her SIA team, preferably through stakeholder consultation, should identify all possible negative societal impacts, who these will impact, and their likelihood (frequency) and consequence (magnitude of impact) as well as the numbers of people who could be affected. Often, the best way to identify these impacts is to consider the principles associated with each type of societal impact and/or a set of questions which can help identify negative societal impacts, as provided in Section 2.1. The assessor will benefit from engaging stakeholder representatives and experts to have their views. The assessor, other members of the SIA team and stakeholders consulted should raise other questions that can help to identify the societal impacts of the proposed project. Table 5 demonstrates how an assessor should use the spiral methodology and approach the six relevant sectors in three phases.

It should be noted that 'impacts' are not solely negative, and part of this approach includes the assessment of potential benefits from security research (including, for example, impacts on welfare, growth and competitiveness). This is particularly the focus of assessment round 1: ensuring security research meets the needs of society. This is not just a threshold check, but an opportunity for better understanding the pathways to desirable beneficial outcomes.

Deciding how to mitigate or eliminate or avoid or transfer negative societal impacts is also a somewhat political decision as is the decision regarding which benefits to pursue. The assessor or project manager or organisation may decide that the benefits of the project or technology outweigh the perceived negative impacts arising from its development and deployment. SIA should be regarded as part of the organisation's risk management, although this should be balanced against the need to actually learn through the process. In order to facilitate socially robust innovation, it could be argued, SIA needs to provide room for genuine learning on the side of all actors involved, and the possibility that core policies and plans will be aborted or reformulated needs to remain a possibility.

The organisation should maintain an impact register, in which the assessor (and/or other organisation employees) identifies the impacts, their seriousness, what the organisation has decided (if anything) to do about them, who is the person responsible for managing it. The impact register should be regularly updated (e.g. every six months or at appropriate milestones in the project), depending upon the length of the research project. It is important to include all

Table 5. Assessment phases

	Way of life, fears and aspirations	Culture and community	Political systems	Environment	Health and wellbeing	Personal and property rights
Assessment Round 1: Ensuring security research meets the needs of society						
Which documented societal security need(s) does the proposed research address? (e.g. life, liberty, health, employment, property, environment, values)						
How will the research output meet these needs? How will this be demonstrated? How will the level of societal acceptance be assessed?						
Is the research project aware of challenges to these needs?						
Does addressing the documented societal needs through the proposed research require any trade-offs with other documented societal needs? How is this trade-off decided? Is this trade-off still valid if the research is less effective than anticipated?						
What threats to society (e.g. crime, terrorism, pandemic, natural and man-made disasters) does the research address?						
How is the proposed research appropriate to address these threats?						
What other measures could be adopted to address these threats?						
Assessment Round 2: Ensuring security research does not have negative impacts on society						
How could the research have a negative impact on freedom of association?						
How could the research have a negative impact on freedom of expression?						
How could the research have a negative impact on protection of personal dignity?						
How could the research have a negative impact on privacy and data protection?						
How could the research have a negative impact on property rights?						
How could the research have a negative impact on access to public space?						
If implemented, how could the research have a negative impact on this aspect (culture and community, way of life etc.)?						
How could the research impact disproportionately upon specific groups or unduly discriminate against them?						
Could the research have impacts upon vulnerable groups (including, but not limited to: the elderly, the disabled, children and young adults, homeless people, economically disadvantaged people and people in precarious situations, immigrants or non-citizens, and lesbian, gay, bisexual, transgender or queer identifying people)?						
How could the research increase discrimination?						
Assessment Round 3: Ensuring security research benefits society						
What segment(s) of society will benefit from increased security as a result of the proposed research?						
How will they benefit?						
Are additional measures required to achieve this benefit?						
Are additional measures possible to extend these benefits to other segments of society?						
In what contexts might this benefit be lacking or not be delivered by the research project?						
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 and transparency; strengthened community engagement, human dignity; good governance; social and territorial cohesion; sustainable development?						

identified impacts in this register even if they are accepted at later stages in the process.

2.2.2.4 Formulate recommendations. Based on her analysis of the societal impacts, the assessor should prepare a set of recommendations, which will form part of the SIA report. The assessor should be clear to whom her recommendations are directed: some could be directed towards different units within the organisation, some to the project manager, some to the CEO, some to employees (including researchers) or employee representatives (e.g. trade unions), to regulatory authorities etc. The assessor should provide the rationale for each of her recommendations. The recommendations could include procedural and more general organisational matters (e.g. relating to training and raising awareness and accountability) as well as those relating specifically to societal impact.

Potential venues and options for the publication of research findings (e.g. open-access publication) can be identified at this stage as they will contribute to the positive societal impacts of the security research.

2.2.3 Reporting and responding

2.2.3.1 Prepare and publish the report. The assessor should prepare her SIA report, and the organisation should publish it on its website and/or submit it to an appropriate repository. An outline and recommended contents of a SIA report are provided in Section 3 of this paper. Research funding bodies may have specific reporting requirements for SIA exercises.

Some organisations may be reluctant to publish their SIAs because they fear negative publicity or they have concerns about competitors learning something they do not want them to. Such concerns seem overdone.

Publication offers many benefits and opportunities to the organisation. It demonstrates that the organisation treats societal issues seriously, and consequently its customers or citizens. Customers and citizens are more likely to invest their trust in an organisation that treats their wellbeing, environment, individual rights and other concerns with respect. It offers an opportunity to gather additional feedback from stakeholders. It offers the organisation an opportunity to distinguish itself from its competitors. For organisations concerned about publishing commercially sensitive information or security sensitive information, there are solutions. The organisation can simply redact the sensitive parts or put them into a confidential annex or just publish a summary of the project or, if necessary, provide a copy to the regulator.

2.2.3.2 Implement the recommendations. The project manager and/or the organisation does not need to accept all these recommendations, but they should say which recommendations they have implemented already or intend to implement and which they do not intend to implement and the reasons why they do not intend to do so. The organisation's response to the assessor's recommendations should be posted on the organisation's website. This transparency will show that the organisation treats the SIA recommendations seriously, which in turn should show consumers and citizens that the organisation merits their trust. The organisation should put in place a mechanism or system for updating the SIA report as necessary and, especially, for monitoring the implementation of the recommendations.

Research funding and support institutions may also wish to be informed of how a research institution is implementing the recommendations.

Recommendations from the SIA may have implications for the research methods and research design used in a security research project.

2.2.3.3 Ensure a third-party review and or/audit of the SIA. The value of independent third-party review or audit has been established for PIAs, in term of guaranteeing quality and rigour (Stoddart 2013). This is likely to hold true for SIAs. For research projects this review will need to planned for in advance, with appropriate third parties identified. Existing review bodies, for example research funding agencies, will have their own evaluation and reporting requirements, which may support the external review of the SIA, but these agencies may not yet have the capacity to fully audit the SIA process.

2.2.3.4 Update the SIA if there are any changes in the project. Many projects undergo changes before completion. Research on technological development may go in several different directions before achieving its goal. Research with a social dimension may also uncover previously unidentified societal impacts. Whenever material changes occur, the project manager and/or assessor should revisit the SIA to see whether it needs to be amended, which will almost certainly be the case where new societal impacts become apparent that were not previously considered. The value of the spiral methodology is that it highlights the importance of revisiting key questions through the lifetime of the project, and holding initial findings contingent. Depending on the magnitude of the changes, the assessor may need to revisit the SIA as if it were a new initiative, including a new consultation with stakeholders.

2.2.3.5 Refer to the SIA in any post-project evaluation. The SIA process does not end with the publication of the report, but should be continued into any evaluation work related to the security research project. Depending upon the scope and scale of the project, additional resources and methods may be available to evaluate the efficacy of the security research or applied security measure, these activities should include a consideration of societal impact.

3. The SIA report

A SIA will have several key outcomes. For example, a key outcome will be the identification and overcoming of any negative societal impacts. Another outcome will be the benefits of stakeholder interaction and engagement. Yet another outcome will be the discovery of new knowledge and learning (by the organisation as well as others). Still another key outcome of this methodology will be a SIA report for the security research project. This section of the paper provides guidance on the contents and purpose of the societal impact report. The report documents the assessment process, and contains the resulting findings. It acts as a reference document during the conduct of the project and as part of evaluation work afterwards. The report can serve both as evidence and a record of the SIA process. It can serve as a touchstone during the project for project staff and other participants, and as a way to demonstrate commitment to understanding and managing societal impacts of the project.

This reporting guidance draws upon the structure of privacy and SuIAs (Wright and Wadhwa 2012), as combined with the influences of CTA and SIAs, and configured for application to societal impacts of security research. This section describes the structure of the final, completed report. However, several sections of the report, particularly those related to background, planning and project description, should be initiated in the planning and preparation stage detailed above.

The report should contain the following sections:

(1) background and identifying details
(2) introduction and overview of the SIA process
(3) project description
(4) societal impacts
(5) options and alternatives
(6) design features to manage societal impacts
(7) compliance with laws, regulations, codes and guidelines
(8) stakeholder analysis and result of consultation(s)
(9) recommendations

1 Background and identifying details. The SIA report should state on its cover page at least the following elements:

- SIA on [name of the project]
- name and address of the organisation sponsoring the SIA
- contact person (the assessor), title and email address
- date of the SIA report

The length of the SIA report may justify an executive summary, which should state why the SIA was undertaken, who initiated the SIA and who conducted it. The executive summary should provide a brief description of the security research project or technology application that was the subject of the SIA. It should say which stakeholders (or stakeholder groups) were consulted. It should identify the principal societal impacts, across the six categories and the alternatives for minimising or avoiding negative impacts. The summary should contain the principal recommendations of the SIA report.

The SIA report should include a section that describes how senior management is involved in decision-making related to societal impacts of security research. Does the senior management board regularly discuss the impacts of security research or applied security measures? Are there specific office holders whose responsibility includes societal impacts?

This background section should identify any organisational issues that are directly or indirectly implicated by the development of the project. For example, it may become apparent that the development of the project requires putting in place an organisational mechanism for ensuring accountability, for instance, that the CEO or her designated senior manager is responsible for ensuring that the development of the project does not negatively affect the organisation or stakeholders, and that beneficial societal impacts are maximised. The organisation should have procedures in place whereby funding for the proposed project is tied to completion of a satisfactory SIA beforehand.

2 Introduction and overview of the SIA process. The introduction section should outline the scope of the SIA, when, why and for whom it was performed, and by whom. It should provide initial information about the project or security measure assessed. It should introduce the methodology employed in the SIA, which can be drawn from Section 2.1 of this paper, or adapted as required. Adaptations should, however, be documented. It should also set out the terms of reference for the assessment.

This section should describe the SIA process undertaken (similarly, this can be drawn from Section 2.3) and what was the outcome of each stage of the process. It should describe the scale of the SIA undertaken and why the organisation developing the project and (presumably) sponsoring the SIA felt the scale of the SIA undertaken was appropriate. It should refer to any stakeholder consultations undertaken and the approach adopted to support these.

This section of the report should also describe any measures that have been undertaken to attempt to increase the role of stakeholders in decision-making processes relating to the research project or security measure implementation.

3 Project description. This section should provide a detailed description of the project including its objectives and justification for the project. This should include initial answers to the societal needs questions from Section 2.1 and can assist with project planning.

Details of the project can be added as the SIA progresses, as the spiral expands and greater knowledge regarding societal impacts is produced.

This section should include information on the documented societal needs to which the security research or application is addressed, and how the project will address these needs. It should contextualise the project against its theoretical background and core assumptions.

This section should also state the main aims of the project or technology? Why is this research being conducted (or proposed) and the system or technology being established? What are the principal features of the security measure proposed?

The project description should state who is undertaking the development of the project, and when it is expected to be conducted or deployed. It should state the subject of the project, potential beneficiaries, and stakeholders who might be interested in or affected by the project.

The project description should provide some contextual information about how the project fits with the organisation's other services or activities. It should state whether aspects of the project are, or will become, proprietary. It should indicate the intended outcome of the project (e.g. fundamental scientific advances, a new technology, a demonstrator or a commercial product or service).

4 Societal impacts (risks). This section should list and describe the societal impacts posed by the project. Thus, the organisation or project manager or assessor should

consider the impacts of the proposed project on all six categories of societal impact identified above. This section can set out the responses to the questions from Section 2.1. These reflections in initial drafts of the reports can be expanded upon in later and final versions as more information is produced by investigation and consultation. The assessor should state how she and/or the organisation believe the impacts will affect the project objectives.

5 Options and alternatives. The SIA report should include a section that identifies the options and alternatives available to the organisation in order to mitigate, avoid, transfer, eliminate or accept the negative societal impacts identified by the SIA, as well as those that could optimise the realisation of societal benefits. The report should say why particular options or alternatives were rejected or discounted and why a particular course of action has been recommended. If the organisation has decided to proceed with the research project or technology implementation despite the SIA raising the risk of negative societal impact, the assessor should say (if she knows) how the organisation justifies these. Opinions and alternatives should be understood broadly to also include alternative policy directions.

6 Design features to manage societal impacts. This section should describe the design features adopted within the project or technology application to reduce or avoid negative societal impacts and to maximise positive societal impacts, and state what the implications of these design features are (e.g. how they affect the viability of the project). The report could include a table like the one in Table 6.

Table 6. Societal impact response table

Societal impact	Category	Description	Mitigation/ benefit maximisation measures	Implications for project
	Way of life, fears and aspirations			
	Culture and community			
	Political systems			
	Environment			
	Health and wellbeing			
	Personal and property rights			

7 Compliance with laws, regulations, codes and guidelines. The SIA report should identify the laws, regulations, codes of conduct and guidelines with which the project complies or should comply.[7] This section should also provide an assessment of whether the security research has the potential to generate results that require new legislation to address potential gaps. For example, if a new technology were to drastically improve the surveillance capacity of an existing technology, perhaps by removing any possibility for anonymity in public space, would this require revision of data protection legislation? In addition, this section should state how the organisation monitors compliance with the laws, regulations, codes of conduct and guidelines it has identified.

8 Stakeholder analysis and results of the consultation(s). The report should identify who are the principal stakeholders interested in or affected by the project, and how the assessor or the organisation arrived at this list. The report should specify what efforts the organisation has made to consult with stakeholders, including the public, to gather their views and ideas about potential societal impacts, how they might be affected by the project (positively and/or negatively) and how negative impacts could be mitigated, avoided, minimised, eliminated, transferred or accepted. The assessor should specify which consultation techniques were employed (surveys, interviews, focus groups, workshops, conferences, Delphi, surveys etc.), when they were undertaken, the results of each consultation exercise and whether differences in opinions were discovered when different techniques were used. If any particular stakeholder consultation tools were used in the process, this should also be noted.

The assessor should state who was consulted and what information materials the organisation provided to stakeholders, including the public. Such materials might be included as an annex to the report. The assessor should state whether the consultations yielded any new findings and what efforts the organisation has made to take into account stakeholder views and ideas in the design of the project. Did any fundamental changes result from stakeholder consultation? The assessor should state how she views public acceptance of the project (Does the public accept the project? Or not? Or is opinion divided? Or does anyone care?).

9 Recommendations. The assessor should set out her recommendations, which could be a few or many, depending on the case. They could be detailed and specific or high-level. The recommendations are primarily aimed at reducing or removing negative societal impacts and increasing positive societal impacts. Some negative impacts may, on balance, be worth accepting and, if so, the assessor should explain why. The assessor should be

clear who will bear the negative and positive impacts (Will it be society, specific social groups, the organisation conducting the project, stakeholders, suppliers or others?).

The assessor should also set out what further work is necessary or desirable with regard to the SIA. For example, the assessor should make recommendations with regard to the need for independent third-party monitoring of implementation of the recommendations.

The assessor should also make recommendations as to whether the SIA report should be made public. The default mode should be to make the SIA report public (e.g. to post it on the organisation's website), however, there may be circumstances where it might not be appropriate to make the SIA or parts of it public (e.g. there may be security, commercial-in-confidence or other competitive reasons). Often the report can be redacted in places and then made public or sensitive parts can be placed in a confidential annex.

4. Conclusions and recommendations

An SIA should be completed for all security research, and lessons learnt from PIAs, SuIAs, CTA and SIA to ensure that high standards are met in terms of real assessment, and to prevent SIA becoming a box-ticking exercise. A coherent methodological approach and structured processes, integrated with existing research practice, combined with clear reporting should contribute to minimising negative societal impacts and increasing the positive societal benefits of security research. The structured methodology presented here provides guidance through such a process.

Whilst benefits can be achieved by security researchers and security research organisations conducting SIAs, additional benefits can be achieved by mainstreaming such assessments within wider security research contexts. Options for achieving this include: integrating SIA into research frameworks, gaining the support of research support institutions and policy-makers, sharing expertise and providing training in SIA, and collating together evidence of the benefits of SIA activities.

SIA methodologies and guidance could be trialled in the European Commission's Horizon 2020 Secure Societies work programme (which lists various calls for security proposals), mirroring the deployment of the Societal Impact Working Group checklist. However, as the SIA approach builds upon that checklist, and adds a structured methodology for assessing and reporting upon societal impact, the Societal Impact Working Group work could stand a precursor, allowing a more rapid adoption of SIA. Many research actors will have some measure of experience with the preceding approach, upon which this builds. Deployment of SIA with large-scale research frameworks will help to achieve the policy objectives of secure societies without infringing uponfundamental values. Such an effort would require the support of the organisations responsible for such frameworks such as the EU's Research Executive Agency. The Social Impact Measurement Working Group identified the following phases, into which SIA might be implemented: work programmes and annual calls (setting the security research funding framework), proposals (the exercise of putting together a research proposal and responding to the funding framework), negotiation (between funders and researchers, and involving the alteration of the research proposal to fit the framework), project execution, and the implementation of a completed product, system or technique in different contexts (McCarthy 2012: 11).

Training in this methodology could be supported by institutional funding bodies, research prioritisation agencies, research institutions and other appropriate actors. This would increase the capability, skill level and experience of security researchers, across a broad range of organisations, in the conduct of SIA. This training could be supported by developing a network of practitioners with expertise in SIA. This network would act as a resource and store of experience for conducting SIAs. It would also facilitate organisations seeking advice or looking to include SIA in their research activity, either on a contractual basis, or through partnerships. The network of practice could also collate SIA reports and examples of good practice in SIAs. This would contribute towards building an evidence base for the ability of SIA to increase the positive societal impactsof security research and decrease the negative impacts, as well as providing future research projects with models of how to achieve this. It would also facilitate analysis of long-term security research funding frameworks as a whole, including the ability to reflect upon the societal impact of agenda setting.

Funding

This work was supported by the European Commission Framework Programme 7-Security Programme, Sub-programme SEC-2012.6.3-2 [Project reference 313062].

Acknowledgements

This paper draws upon research conducted within the ASSERT project (<www.assert-project.eu>). The authors owe particular thanks to Barbara Prainsack, Lars Ostermeir and Inga Kroener, as well as the participants at the ASSERT project Societal Impact Assessment Masterclass held at the University of Stirling, UK in February 2014.

Notes

1. See Lee and Kirkpatrick (2006) for an early review of this process.

2. The term 'spiral curriculum' was originally suggested by Bruner (1960).
3. Vanclay separates culture from community, as well as way of life from fears and aspirations, however, we believe that a smaller number of categories is sufficient to cover these issues while at the same time striking a balance between addressing different issues and useability.
4. In the course of the SIA, it may become apparent to the assessor that the organisation needs to spend more time on raising the awareness of employees (including researchers) about societal impact issues. The background context section of the report can be used to state what the organisation does now to raise employee awareness of societal impacts, and where it could improve.
5. For a longer list of possible techniques, see OECD (2004: 30–2 (Box 2. Commonly cited techniques for informing deliberation through stakeholder involvement)).
6. See <http://securitydecisions.org/about-dessi/, and http://www.siam-project.eu/> accessed 7 Jul 2014.
7. PIA in the EU is conducted with reference to the Data Protection Directive 95/46/EC, the E-Privacy Directive 2002/58/EC and the Data Retention Directive 2006/24/EC. Because SIA takes into account a broader range of potential impacts, it must also take into account a correspondingly wider range of legislation.

References

Bishop, P. and Davis, G. (2002) 'Mapping public participation in policy choices', *Australian Journal of Public Administration*, 61: 14–29.

Braun-Thürmann, H. (2005) *Innovation*. Bielefeld, Germany: Transcript Verlag.

Bruner, J. (1960) *The Process of Education*. Cambridge, MA: The President and Fellows of Harvard College.

Buzan, B. and Hansen, L. (2009) *The Evolution of International Security Studies*. Cambridge UK: CUP.

——, Weaver, O. and de Wilde, J. (1998) *Security: A New Framework for Analysis*. London: Lynne Rienner.

Chilton, P. (1996) *Security Metaphors: Cold War Discourse from Containment to Common House*. New York: Peter Lang.

European Commission. (2013a) 'Key procedural steps for the Commission/smart-regulation/impact', 20 December 2013 <http://ec.europa.eu/smart-regulation/impact/ia_key/ia_key_en.htm> accessed 7 Jul 2014.

—— (2013b) 'Secure Societies – protecting freedom and security of Europe and its citizens', <http://ec.europa.eu/programmes/horizon2020/en/h2020-section/secure-societies-%E2%80%93-protecting-freedom-and-security-europe-and-its-citizens> accessed 29 Jan 2014.

—— (2013c) *'Special Barometer 401: Responsible Research and Innovation (RRI), Science and Technology Report*, European Commission.

—— (2014) 'Smart Regulation', 13 January 2014 <http://ec.europa.eu/smart-regulation/index_en.htm> accessed 29 Jan 2014.

European Parliament, Council and Commission. (2010) 'Charter of Fundamental Rights of the European Union', 2010/C 83/02, *Official Journal*, 30.3.2010 <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0389:0403:en:PDF> accessed 7 Jul 2014.

European Security Research Advisory Board. (2006) 'Meeting the challenge: The European Security Research Agenda', <http://ec.europa.eu/enterprise/policies/security/files/esrab_report_en.pdf> accessed 7 Jul 2014.

Genus, A. (2006) 'Rethinking constructive technology assessment as democratic, reflective discourse', *Technology Forecasting and Social Change*, 73: 13–26.

Guillemin, M. and Gillam, L. (2004) 'Ethics, reflexivity and "ethically Important" moments in research', *Qualitative Inquiry*, 10: 261–80.

Kemp, D. (2011) 'Understanding the organizational context'. In: Vanclay, F. and Esteves, A. M. (eds) *New Directions in Social Impact Assessment: Conceptual and Methodological Advances*, pp. 20–37. Cheltenham, UK: Edward Elgar.

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

Lianos, M. (2000) 'Dangerization and the end of deviance: The institutional environment', *British Journal of Criminology*, 40: 261–78.

McCarthy, S. (2012) *Report of the Societal Impact Expert Working Group: EC DG ENTR Report*. Brussels: European Commission.

Mason, J. (1996) *Qualitative Researching*. London: Sage.

Müth, M. (2003) *Verkherspolitik in Metropolen Südostasiens*, (Transl.: The politics of traffic in South East Asian Metropolis areas). Hamburg, Germany: Abera.

Neocleous, M. (2007) 'Security, liberty and the myth of balance: Towards a critique of security politics', *Contemporary Political Theory*, 6: 131–49.

Nissenbaum, H. (2009) *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford, CA: Stanford Law Books.

OECD. (2004) *Stakeholder Involvement Techniques*. Paris: OECD, <http://www.oecd-nea.org/rwm/reports/2004/nea5418-stakeholder.pdf> accessed 7 Jul 2014.

O'Faircheallaigh, C. (2010) 'Public participation and environmental impact assessment: Purposes, implications and lessons for public policy making', *Environmental Impact Assessment Review*, 30: 19–27.

Peterman, W. (2004) 'Advocacy vs. collaboration: Comparing inclusionary community planning models', *Community Development Journal*, 39: 266–76.

Rip, A. and Schot, J. (1997) 'The past and future of constructive technology assessment', *Technological Forecasting and Social Change*, 54: 251–68.

—— and —— (2002) 'Identifying loci for the influencing the dynamics of technology development'. In: Sorensen, K. H. and Williams, R. (eds) *Shaping Technology, Guiding Policy: Concepts, Spaces and Tools*, pp. 155–72. Cheltenham, UK: Edward Elgar.

—— and van Lente, H. (2013) 'Bridging the gap between innovation and ELSA: The TA program in the Dutch Nano-R&D Program Nano Ned', *Nanoethics*, 7: 7–16.

Russell, W. A., Vanclay, F. M. and Aslin, H. (2010) 'Technology assessment in social context: The case for a new framework for assessing and shaping technological developments', *Impact Assessment and Project Appraisal*, 28: 109–16.

Schot, J. and Geels, F. W. (2008) 'Strategic niche management and sustainable innovation journeys: Theory, findings,

research agenda and policy', *Technology Analysis and Strategic Management*, 20: 537–54.

Stoddart, J. (2013) 'Auditing privacy impact assessments: The Canadian experience'. In: Wright, D. and de Hert, P. (eds) *Privacy Impact Assessment*, pp. 419–36. Dordrecht, the Netherlands: Springer.

United Nations. (5 April 2012) Follow-up to General Assembly resolution 64/291 on human security: Report of the Secretary-General, <https://docs.unocha.org/sites/dms/HSU/Publications%20and%20Products/Reports%20of%20the%20Secretary%20General/A-66-763%20English.pdf> accessed 20 Jan 2014.

Vanclay, F. (2003) 'International principles for social impact assessment', *Impact Assessment and Project Appraisal*, 21: 5–12.

—— and Esteves, A. M. (2011) 'Current issues and trends in social impact assessment'. In: Vanclay, F. and Esteves, A. M. (eds) *New Directions in Social Impact Assessment: Conceptual and Methodological Assumptions*, pp. 3–19. Cheltenham, UK: Edward Elgar.

Wright, D. (2012) 'The state of the art in privacy impact assessment', *Computer Law and Security Review*, 28: 54–61.

—— (2013) 'Making privacy impact assessment more effective', *The Information Society*, 29: 307–15.

—— and de Hert, P. (2012) 'Introduction to privacy impact assessment'. In: Wright, D. and de Hert, P. (eds) *Privacy Impact Assessment*, pp. 3–33. Dordrecht, the Netherlands: Springer.

—— and Raab, C. (2012) 'Constructing a surveillance impact assessment', *Computer Law and Security Review*, 28: 613–26.

—— and Wadhwa, K. (2012) 'A step-by-step guide to privacy impact assessment', Paper presented at Second PIAF Workshop, held Sopot, Poland, 24 April 2012 <http://www.piafproject.eu/ref/A_step-by-step_guide_to_privacy_impact_assessment-19Apr2012.pdf> accessed 7 Jul 2014.