ASSERT Report Summary

Project reference: 313062
Funded under: FP7-SECURITY

Periodic Report Summary 1 - ASSERT (Assessing Security Research: Tools and Methodologies to measure societal impact)

Project Context and Objectives:
That there is a strong societal dimension to the products developed by the European security industry is an appraisal that has become almost commonplace. Yet there is, to date, no systematic institutional approach to tackling unintended (and usually negative) consequences of technologies that display a high likelihood to undermine the security of society as a whole. Also, there has been insufficient support for researchers on how to carry out SIA in the practical context of a concrete project proposal.
ASSERT started in a context where no clear ideas existed about the principles governing an approach that would lead to better choices regarding technology development in security research: while
Project No.: 313062
Period number: 1st
Ref: 313062_ASSERT_Final_Report-11_20140815_193321_CET.pdf
Page - 3 of 26
indeed, the societal dimension was seen as critical, this happened predominantly to the extent that such societal consideration would increase the acceptability of technological solutions and thus help open up markets (e.g. in the 2012 European Commission's Action Plan on Security Industrial Policy (European Commission, 2012)). SIA in such an understanding would move to a position where it could be used as a 'legitimacy apparatus' to help sell technology. In contrast, ASSERT positioned SIA as an approach to be endowed with powers in its own: SIA should lead to the reframing of project objectives and envisaged results, especially if the assessment leads to the discovery of negative consequences of the proposed research. Conceiving of a mechanism with such potential is very different from ideas about impact assessment as a tool to create legitimacy for research projects. In order to contribute a more systematic approach to assessing the impacts of security research activities, ASSERT pursued these objectives:
• Survey and analyse traditions of impact assessments beyond security research in order to develop best practice criteria;
• Closely investigate the extent to which these best practices could be transferred and applied to the field of security research;
• Contribute to the establishment of an expert community in societal security by establishing an online expert database and the concept of a "Masterclass in Societal Security";
• Provide guidance for stakeholders engaged in impact assessment;
• Develop and offer an online repertory which delivers both theoretical inputs as well practical training modules
The subsequent sections show how these objectives were met and what the tangible outcomes of the ASSERT project are.
To achieve its objectives ASSERT relied on the following working structure:
• WP1 (What is societal impact?)
o Provide an overview of current good practices of the exploration and assessment of the societal impact of broader areas of science and technology, with a particular focus on innovative and deliberative approaches;
o Assess the extent to which these good practices are feasible and useful to security technology research.
• WP2 (Who are the relevant actors?)
o Identify and create a pool of experts with knowledge about the societal impacts of security policy and practice;
o Provide a user-friendly knowledge base (an online communications tool and database) to assist the European Commission in implementing the recommendations of ASSERT and other relevant research relating to assessing the societal impacts of security research, policy and practice.
• WP3 (How can we provide practical guidance to the relevant actors?)
o Develop and test tools and methodologies to assess and mainstream the societal impact of security research;
o Develop an online assessment tool for determining societal impact;
o Provide hands-on guidance for planning and implementing a SIA process.
One of the main challenges with strengthening the role of societal security and related impact assessment mechanisms is the identification of relevant actors and of ways to engage them. ASSERT structured the field of security research by categorising actors according to the roles they typically play in setting the agenda for research programming and project execution, but also for adopting research results and thereby facilitating the impact of research results. This categorisation helps to better understand the ways in which ASSERT approached the field and is

presented in the Annex to this report. It also depicts potential intervention points across the innovation journey (from programme planning to programme evaluation) where results could create impact. The matrix plots the relevant stakeholders (Policy Makers, Evaluators, Members of the Programme Committee, Researchers and Research Organisations, Civil Society Organisations and End-Users of security research against relevant intervention points: Setting the Agenda, Distributing Resources, and Creating a sustainable research impact.
Project Results:
ASSERT, being a Coordination and Support Action, consists of one reporting period. Therefore, the results covered here do not differ from those described in the Final Report.

WP1 was tasked with screening the relevant academic and policy fields for state- of-the-art best practices. This means that research was carried out on the origin, as well as the main conceptual and methodological underpinnings and commitments of SIA, CTA, PIA and SuIA more generally, instead of being limited to only those aspects that pertain to the assessment of research.
Social impact assessment is probably the oldest of all impact assessments. In its dominant current iteration, it is understood as

“the process of analysing, monitoring and managing the intended and unintended consequences, both positive and negative, of planned interventions [...] and any social change processes invoked by these interventions” (Vanclay 2003, 2006).

For a better understanding of the methodologies used throughout all assessment practices, an extensive literature review was carried out in WP1. As outlined in the WP1 deliverables, especially Esteves et al. (2012: 35; adapted from Vanclay & Esteves 2011) contributed to a better understanding of the state of the art in impact assessment. Good impact assessment includes the following elements: 1. creating participatory processes and deliberative spaces to facilitate community discussions about desired futures, the acceptability of likely impact and proposed benefits, and community input into the SIA process;
2. gaining a good understanding of the communities likely to be affected by the policy, programme, plan or project including a thorough stakeholder analysis to understand the differing needs and interests of the various sections of those communities;
3. identifying community needs and aspirations;
4. scoping the key social issues (the significant negative impacts as well as the opportunities for creating benefits);
5. collecting baseline data;
6. forecasting the social changes that may result from the policy, programme, plan or project;
7. establishing the significance of the predicted changes, and determining how the various affected groups or communities will likely respond;
8. examining other options;
9. identifying ways of mitigating potential impacts and maximising positive opportunities;
10. developing a monitoring plan to inform the management of change;
11. facilitating an agreement-making process between the communities and the developer ensuring that principles of free, prior and informed consent (FPIC) are observed and that human rights are respected, leading to the drafting of an impact and benefit agreement (IBA);
12. assisting the proponent in the drafting of a social impact management plan (SIMP) that puts into operation all benefits, mitigation measures, monitoring arrangements and governance arrangements that were agreed to in the IBA, as well as plans for dealing with any ongoing unanticipated issues as they arise;
13. putting processes in place to enable proponents, government authorities and civil society stakeholders to implement arrangements implied in the SIMP and IBA and to develop their own respective management action plans and embed them in their own organisations, establish respective roles and responsibilities throughout the implementation of those action plans, and maintaining an ongoing role in monitoring.
Of critical relevance for all assessment approaches is the question of participation in the process of agenda setting and programme shaping. O’Faircheallaigh (2010) points to the questions of power differential by differentiating between public ‘participation as input for decision makers’ (in the sense of ‘consultation’) on the one hand, and ‘public participation in decision making’ [emphasis added]. Thus, agency of the various actors needs to be discussed and determined. Prainsack (2014) has developed a grid to address the challenge of analysing the participation in an assessment project, including 19 relevant points:
Coordination: Who has influence in:
1. Agenda setting
2. Determining the terms of the execution of the idea, and procedural aspects
3. Deciding what results are (and what ‘good’ results are)
4. Deciding what will be done with results
5. Deciding on intellectual property questions
Participation
6. Who participates (demographic and social parameters of those who participate)? Why, and how do they participate?
7. How much, and what kind of, training, skill, or expertise is required to participate in this project? 8. Are there cultural, institutional, or other differences in perception and framing of core issues and stakes?

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

Evaluation:
10. How and by whom is it decided what good outcomes are?
11. What happens to the results of these evaluations?
Openness and information symmetry:
12. Do participants in the project have access to the core data about the project?
13. Can participants in the project edit or change the core datasets?
14. Is the contribution of participants adequately acknowledged in published materials, and policy briefing documents, etc?
15. Are datasets made publicly accessible (open source or open access)?
16. Are main findings made publicly accessible (open source or open access)? Are assessment reports made publicly accessible?
Entrepreneurship:
17. How is the assessment project funded?
18. What is the role of for-profit entities in this assessment project? Are these small, medium-sized, or large entities, and where are they located?
19. How are for-profit and other interests aligned in this assessment project (and/or do they conflict, and where?)

Transferring best practice cases to the field of security research:
One challenge that seems to be crucial is the creation of an awareness for societal dimensions and for how they impact R&D processes, whether this is explicitly recognised or not. In most domains of R&D planning and evaluation, some forms of consultative processes are already in place, but those are rarely labelled as SIA procedures. A challenge is then to raise the awareness of the potential to enhance existing procedures in many institutions by more systematically planning and conducting SIA procedures. A starting point for this could be to distinguish different phases of the R&D process and then to define how SIA could impact on the process at the different phases and what the means are to achieve the desired impact. This has been done in WP1 (Ostermeier 2013). The matrix is included in the Annex to this report.

1. Clarify how security is understood in a given project (especially when this is implicit)
How does the project enhance the security of European citizens and societies? What types of security (environmental, health, national, energy security, etc.) are implicit or explicit in the project? Whose security is enhanced – and whose security is not? What are alternative measures that could lead to the same enhancement of security?
2. Clarify what kind of societal impacts could be relevant in the context of a particular project Impacts can include a wide range of benefits, harms, unintended (structural) consequences, etc. on individuals, minorities, households, enterprises and communities. Advantages and disadvantages can be distributed unevenly, i.e. distinguish who benefits from the projects, and who endures the drawbacks. Ensure that complex societal challenges are not reduced to issues that can be fixed with technological solutions only.
3. Findings from SIA should have the potential to adapt the project and R&D process
SIA should not be an “add-on” at the end of the project, but it should be integrated into the project at its earliest stages, and have the possibility to modify the project in case significant undesirable impacts are anticipated. Project proposals should show how they plan to react to these impacts, which usually requires some flexibility in project implementation and the capacity to amend project plans.
4. Participation of relevant people and groups means more than merely to inform or consult them. Also, engagement with wider groups than only end users may be necessary
Stakeholders, users, or members of the public can be important sources of knowledge on likely societal impacts. Depending on the nature of the project, they can be integrated into different stages of the project. Merely asking them once for the sake of “ticking the box” of user engagement is typically not satisfactory. The range of people or communities affected by a project may be much wider than end users. Engaging stakeholders as far as possible into the decision-making process is desirable and a way of reducing risks. The extent to which stakeholders should be informed, consulted or engaged depends on the likelihood and severity of the societal impacts as well as their particular vulnerability. A project with major impacts will need a more rigorous engagement strategy than one that has minimal or no such impacts. Similarly, the range of stakeholders also depends on the likelihood and severity of impacts. Weak and vulnerable (minority) groups often require a more pro-active approach and engagement.
5. Keep the administrative burden reasonable
What is reasonable depends on the project. It is not the case that investing more resources in SIA automatically increases the quality of SIA. Reflexivity is key, not money.
6. Think about transparency and the limitations of the SIA process
SIA can never anticipate all possible impacts. The limitations of SIA should be dealt with in an open and transparent manner. Transparency can also be very useful in various stages of the SIA process itself (e.g. publication of findings of SIA or of impact management plans, etc.). Limitations and shortcomings of the applied SIA should be made explicit.
7. Clarify what purpose the knowledge produced in a SIA should serve
It is important to consider what purpose the SIA should serve. Should it make the project more socially robust? Will it be used to communicate with policy-makers? Is it needed for an evaluation report? Clarifying the purpose of an SIA from the start will help in producing knowledge that is most fit for purpose.

WP2
The main objectives of WP2 were first: to outline the strategy for identifying experts in the field of security research and in particular those with expertise in assessing the societal impacts of security research, policy and practice; second: provide a template for classifying the societal expertise, competences, contact details and institutional

affiliations of the pool of experts in the field of security research, and in particular those with expertise in assessing the societal impacts of security research, policy and practice, and third: the creation of the ASSERT Database of experts in the field of societal security. The ASSERT Database has been designed to 'create a pool of expertise' in societal security, and provides a platform for sharing knowledge and expertise relating to societal security and societal impact assessments, as well as opportunities for capacity and network building. The other main objective of WP2 was to develop and stage a unique training event in societal security and in undertaking a societal impact assessment, known as the ASSERT "Masterclass in Societal Security". The main tool for the objective of building and expert database is the ASSERT Database of Experts in Societal Security http://assert.maisondx.com/lms It is mainly intended for, but not limited to, the actors outlined in the ASSERT description of intervention points (see Annex).
The Expert Database serves several functions, the most important ones are:
• providing a platform for sharing experiences, best practices and expertise,
• Facilitating the emergence of a network with shared interest in developing socially aware security research and policy,
• Providing a pool of experts which can be utilised by the European Commission to shape the governance and design of European research
The underlying objectives for the creation of an expert body are:
• Establishing a community of experts and a platform for sharing knowledge and expertise in societal security;
• Making use of the platform in order to get information about developments around security policy and practice at national or EU level;
• Identifying a body of experts who can assist the EU in the development of EU-funded security research;
• Identifying a body of experts who can assist the EU in the design and evaluation of security research programmes.
The operation of the expert database will be maintained at least one year following the conclusion of ASSERT (i.e. to July, 2015) by STIR.
A core functionality of the ASSERT Database is to support communication amongst expert members and between the membership and the consortium partners and the Commission. Communications will be governed through the ASSERT Data Processing Statement, and the ASSERT Communications Code of Practice (CoP). The CoP relates to all electronic communication supported by the ASSERT Database and Toolkit. It is permanently available on the ASSERT Database and has been circulated to all members of the ASSERT Database. All electronic communication deriving from members of the ASSERT Database assumes prior knowledge and acceptance of the rules contained within the CoP. It sets out the rules governing electronic communication via the ASSERT Database and Toolkit.
Invitations to join the expert database were issued to experts who
• Are known to the consortium;
• Are part of existing academic networks with an interest in societal security, e.g. the Surveillance Studies Network, the Living in Surveillance Societies Network, and other security and surveillance mailing lists;
• Were identified as having participated in security research projects (as listed on the Cordis website);
• Are part of existing policy and stakeholder groups;
• Have previously participated in relevant conferences, such as Computer, Privacy and Data Protection (CPDP) Conference
• Have previously acted as project evaluators for the Commission in the field of security.
In order to reach out the experts, a questionnaire was created that aimed at detailing not only the person's institutional details, but especially their expertise in societal security and previous working/ research experience in this field. The categories used for this were developed by the whole consortium and included:
• Demographic / institutional details • Domains of security activity
o Civil protection
o Defense / intelligence
o Crime & Justice
o Border Security
o Crisis and disaster management
o Critical infrastructure (possibilities to specify the sector mentioned) o Transport
o Financial services
• Areas of security expertise o Privacy
o Data protection / regulation
o Human rights
o Technologies of security and privacy-relevance
• Experience with Societal Impact Assessment
• Membership in a security-relevant academic or stakeholder group
The ASSERT database for experts in societal security is operational. Registration for the database can be done using the link provided at the ASSERT toolkit: http://assert.maisondx.com/?page_id=38. Further information on the purposes of the database and the possibilities it offers can be found at http://assert-project.eu/database-of-experts/ and also in the ASSERT toolkit pages which will be described below in more detail.
Working with the database after registration:
The ASSERT Expert Database can be found at http://assert.maisondx.com/lms It can also be reached from links from the ASSERT Toolkit, the ASSERT project website and the websites of the consortium partners. It has been constructed alongside the ASSERT Toolkit, one of the outputs of ASSERT Work Package 3. Access to the database is 'password protected' with each member of the Database having a unique 'Username' and 'Password'. The ASSERT Database supports a range of functions, these differing according to the designation of those accessing the site, who are either 'managers' or 'members'. Mangers can:
• send messages to individual members,
• send mass messages to all members,

• add/remove users (experts in the Database),
• create accounts and other administrative tasks, • moderate forum discussions, and
• do anything that members can do (see below).

All ASSERT consortium partners have “manager” rights in the database. All experts who registered for membership are “member” by default and have different user rights. Members can:
• Passively receive messages sent by managers via email,
• Actively log-on to the ASSERT toolkit to access an archive of messages,
• create and edit a personal profile in the tool (optionally including information such as affiliations, interests, etc.),
• view the profiles of others,
• send messages to individual members,
• access materials available in the ASSERT Toolkit.
• participate in forum discussions (read and write posts),
• subscribe (and unsubscribe) to forum discussions,
• set their communication preferences (do they want all emails, a daily/weekly digest, no emails etc.), and
• complete administrative tasks, such as resetting passwords.
Currently, the ASSERT expert database has 175 members.
If a member of the Commission, or another appropriate third party wishes to send a message (as a forum message and email) to the members of the expert database, for example, as part of a request for expertise or input, or providing information on issues relating to societal impact of security research, the consortium member organisations would be able to facilitate this. The message can include attached documents. The third party should send a copy of the desired message to the ASSERT coordinator (office@irks.at) who will pass on the message to the group. This intermediary step is required to prevent sending inappropriate messages to the members of the database.
The first ASSERT Masterclass on societal impact assessment was held at Stirling (UK) from 3-4 February, 2014 and involved twenty invited external participants. The idea behind the Masterclass was to provide a structured and participative learning environment for scientists, academics, administrators, evaluators and policy makers that increases their capacity to plan and to manage SIA in the security research domain. The learning outcomes included: securing a good understanding of the concept of societal impact assessment (SIA); the core underlying concepts and theoretical approaches and the different methodologies used to deliver SIA, as well as the perceived benefits and potential barriers to successful SIA; how to put an SIA into practice including methods of constructing an SIA report, with an emphasis on ‘best practice’ criteria, and finally, how an SIA should be integrated with existing organisational procedures and the ways in which existing institutional practices shape the development of an SIA. The participants overwhelmingly enjoyed the Masterclass ‘experience’ and the following is a sample of their comments:
• I found that the masterclass provided a very good introduction into the topic of societal impact assessment. It brought a lot of very interesting people together, people I might have had difficulties to meet otherwise as they are usually not part of my research network (engineering vs. social sciences).
• The organization of the programme with a very good balance between the Masterclass sessions and social activities. The outline of the Masterclass was well structured and the learning outcomes very well-conceived.
• I enjoyed the group activity; interactive learning is always more effective, especially working with others from very different backgrounds.
• The opportunity for networking and exchange ideas with other colleagues from other areas. Being a chemist, it was also useful to be introduced to some areas/techniques of social impact new to me.

ASSERT Deliverable D1.3 provides fuller details of the Masterclass.

WP3
1) Step-by-step guidance on how to plan and implement a Societal Impact Assessment:
With the main objective of operationalising concepts of impact assessment and provide ready-for-use tools, ASSERT WP3 closed a critical gap which hitherto existed in the field of security research as programmed by the EU: before ASSERT, there was no online tool available which could have served to aid in planning and implementing Societal Impact Assessment. WP3 results are essentially the following:
a) Practical guidance for anyone attempting to set up an impact assessment process related to security research:
b) An online toolkit supplying ample theoretical and practical information not only to those charged with planning and designing a SIA for their security research proposal, but also to evaluators and others charged with assessing and evaluating research proposals with regard to the degree to which societal security has been accommodated. This online toolkit also hosts the ASSERT Expert Database described above and an online course management system which was developed and used for the ASSERT Masterclasses. The URL for this is http://assert.maisondx.com.
The SIA-guidance is included in D3.1 and provides a state-of-the art-methodology for conducting a societal impact assessment (SIA) of security research and security measure implementation. Meant as a step-by-step guide, it focuses on several core dimensions of any assessment procedures, which should be understood as a repetitive cycle.
The dimensions are:
• Way of life, fears and aspirations;
• Culture and community;
• Political systems;
• Environment;
• Health & well-being;
• Personal and property rights
The authors of D3.1 provided an illustration to clarify the concept. This illustration is included in the Annex of this report.

One of the main challenges with any assessment project, whether privacy impact assessment, surveillance impact assessment or constructive technology assessment, is that the process may degenerate to a box-ticking exercise. High standards of real assessment have therefore to be met in order to prevent this. Instead, what is required to increase the societal benefits of security research is methodological coherence of the approaches adopted, a good integration of the assessment procedure with existing research practice and clear reporting on the outcomes of the assessment process. This, in turn, will help minimising the negative societal impacts of security research.
2) Online toolkit to support planning and implementing SIA approaches
The ASSERT Toolkit for Societal Impact Assessment in Security Research (http://assert.maisondx.com) is intended to support any assessment procedure for security research or the planning of security measures by creating a knowledge repository on aspects to consider when carrying out or planning assessment procedures. But the toolkit also holds some theoretical elements that help fine-tune and increase quality of the assessment process. Furthermore, the online tool was used by consortium to implement the Masterclass on societal security. The Toolkit is meets several critical design requirements:
The Toolkit is intended to meet the following design requirements:
• Accessibility – use must be straightforward and self-explanatory without complications, information is presented in a logical and structured manner.
• Appealing – present useful information (relevant to its audience and purpose) in a visually appealing manner. Therefore, the toolkit also makes use of interactive elements and multimedia (photos, graphics, video and audio) content. This creates strong added value and synergies with the guidance manual.
• Audience – researchers interested in conducting a societal impact assessment as part of a security research project without significant expertise. Secondary audience: evaluators and funders of security research projects.
• Flexible construction – the tool is adaptable and changeable over time. New content can easily be added, and multiple administrators can update the tool which increases sustainability.
• User-Authentication – the toolkit can differentiate between guests and registered users (as explained above) – and, accordingly, can provide different information to these two groups.
• Support productive learning environment – the toolkit supports and enhances the learning experience of classes and training courses, and it fosters networking activities. The implementation of the ASSERT Masterclass proved that these requirements are also met.
• Host the Expert database – the toolkit hosts the ASSERT Expert database and provides functionality that allows its users to interact and communicate
• Security and privacy protection – the toolkit protects the personal information of registered users and respects their preferences in terms of communications. Access is password protected, the software hosting the platform is updated as updates become available, and the system has system admin responsible for security.
A graphical representation of the structure and composition of the ASSERT online Toolkit is provided in the Annex to this report.

Potential Impact:
In its description of work, the ASSERT consortium pledged to pursue the overall objective of helping to ensure the security of citizens while respecting fundamental rights, including the protection of privacy and personal data, through its development of a social impact assessment methodology applicable to security research. ASSERT has achieved critical results that allow to further pursue this objective:
• D1.2 has elaborated an overview of existing traditions of impact assessment in areas extending beyond security research. It has distilled good practice criteria for planning and conducting such assessments in those areas and empirically validated them in an expert workshop. D1.2 also discusses the transferability of those criteria to the security research domain. Any future attempts to integrate assessments into the research programming and project execution cycle can and should build on the knowledge created in this process;
• D1.3 has elaborated extensively on how the best use of assessment methodologies can be made in the different phases of the research and development process. It builds on empirical findings of an expert workshop organised by Technical University Berlin. D1.3 also lists best practice criteria that were found to be useful by the experts in order to aid future institutional integration of assessment processes. These criteria should serve as the basis for future work that tries to overcome an obstacle that – as of today – still exists: a lack of institutional embeddedness of assessment procedures.
• D1.4 demonstrated how good practice principles can be used to plan and to assess SIAs in different phases of the R&D process. Any future attempts at implements SIA procedures will benefit from those principles that are empirically derived from literature analysis and expert workshops and will help enhance the potential of those SIA processes.
• Future approaches, guided by the ASSERT principles, will have to make sure that the SIA process should have the inherent power to modify goals, categories, and methodologies of the project, and they concern the depth and level of consultation and participation, the flexibility, transparency and iterative nature of the process, the proportionality of the administrative costs incurred by SIA, and the clarity about the goals, limitations, and about the kind of knowledge produced by a specific SIA process
• It seems reasonable to expect that on the basis of the ASSERT good practice criteria, the Commission's 2012 Action Plan for the Security Industrial Policy, which explicitly calls for a better integration of the societal dimension of security technology and a stronger role for impact assessment procedures, could be significantly updated, thereby enhancing its credibility and allowing for more societally inclusive security solutions. One of the main tenets awaiting implementation is to take SIA seriously, which means that the process must be endowed with sufficient power to alter / reframe a project's objectives or envisages outcomes (i.e. moving SIA away from mere tick-box-exercises).
• ASSERT WP2 has designed and constructed a database of experts in societal security. Incorporated into this process was a schema for classifying expertise in the area. This allows for a more comprehensive overview of the different

professional backgrounds and experiences of those active in the field. The classification scheme is built into the profile of experts in the database.
• The ASSERT Database of Experts in Societal Security provides a 'ready-made' pool of experts which can be utilised by the Commission and the Consortium to disseminate knowledge about societal security and other related matters. In doing so, the ASSERT Database provides a platform for enhancing knowledge and facilitating communication about issues relating to societal security. It also allows for the Commission and the ASSERT Consortium to consult the membership of the database on issues relating to societal security. In this respect, the Database serves as a repository of expertise that can be utilised to shape research policy and practice.
• The ASSERT Database and Masterclass' has raised the profile amongst existing researchers of the importance of designing in social impact assessments into existing and future research activity. This aspect of the project has raised awareness amongst a number of researchers planning to submit research project applications in the H2020 funding programme.
• The ASSERT Database and Masterclass has raised awareness of the significance of social issues amongst past and potential future European Commission research evaluators. This will lead to a better understanding of the potential impacts of European H2020 research proposals in the evaluation process. The expert database will have significant impact in fostering the role of societal security in EU-funded security research by making available to the Commission a body of knowledge in this area, and, potentially, even actively engage individual members of the database for advise or assistance in assessing societal impact of security research projects. This will also further develop the current debate and concepts of the Responsible Research and Innovation Agenda.
• The step by step guidance (D3.1) and the online toolkit can be used by future researchers developing a security research proposal and aiming at better considering societal security and cater for potential negative impacts of their project, as well as by future evaluators as part of the process of evaluating such proposals. This guidance has been made easily available and accessible, and supported by relevant templates so that is can be broadly used, even by non-experts.
• A guidance paper was produced for use by the European Commission. Its purpose is to inform evaluators of the ASSERT approach of assessing the societal impacts of security research and increase awareness among evaluators for what needs to be considered when evaluating research proposals. It was produced with the intention to make it available to evaluators at the occasion of the Commission-organised "evaluator information days".
• An article based upon the step-by-step guidance for conducting a Societal Impact Assessment (D3.1) will be published in the journal Science and Public Policy. Hands on practical guidance to the assessment of societal impacts of security research and technology will then be available in a peer reviewed, well established and widely referenced publication.

References used in the report:
Barnard-Wills, David; Wadhwa, Kush, Wright, David (2014): Toolkit for Societal Impact Assessment in Security Research. ASSERT deliverable 3.2 [online]. Available from: Accessed 15 August 2014.
Barnard-Wills, David; Wadhwa, Kush, Wright, David (2014): Societal Impact Assessment Manual and Toolkit. ASSERT deliverable 3.21 [online]. Available from: Accessed 15 August 2014.
Esteves, Ana M.; Franks, Daniel; Vanclay, Frank (2012): Social impact assessment: the state of the art, In: Impact Assessment and Project Appraisal, Vol. 30, No. 1, 2012, pp. 34- 42.
European Commission (2012): Security Industrial Policy Action Plan for an innovative and competitive Security Industry (COM(2012) 417 final). [online]. Available from: Accessed 15 August 2014
ASSERT-Project (2012): Annex I – ''Description of Work'', Fp7-sec-2012-1, Project No. 313062 ASSERT, Assessing security research: Tools and methodologies to measure societal impact.
O'Faircheallaigh, Ciaran (2010): Public participation and environmental impact assessment: Purposes, implications, and lessons for public policy making, In Environmental Impact Assessment Review, Vol. 30, 2010, pp. 19-27.
Ostermeier, Lars; Prainsack, Barbara (2013): Report on good practices of the exploration and assessment of the societal impact of research. ASSERT deliverable 1.3. Available from: Accessed 15 August 2014.
Prainsack, Barbara (2014): Understanding Participation: The 'citizen science' of genetics. In: Barbara Prainsack, Silke Schicktanz, and Gabriele Werner-Felmayer (eds). Genetics as Social Practice. Farnham: Ashgate. 147-164.
Prainsack, Barbara; Ostermeier, Lars (2013): Report on methodologies relevant to the assessment of societal impacts of security research. ASSERT deliverable 1.2. Available from: Accessed 15 August 2014.
Vanclay, Frank; Esteves, Ana M. (eds.) (2011): New Directions in Social Impact Assessment: Conceptual and Methodological Assumptions, Cheltenham, Edward Elgar, 2011.
Vanclay, Frank (2006): Principles for social impact assessment: a critical comparison between the international and US documents, In: Environmental Impact Assessment Review, Vol. 26. No. 1, 2006, pp. 3-14.
Vanclay, Frank (2003): International principles for social impact assessment, In: Impact Assessment and Project Appraisal, Vol. 21, No. 5, pp. 5-11.

List of Websites:
http://assert-project.eu; http://assert.maisondx.com

Related information

Documents and	periodic1-gantt-chart-changing-dates-22052013.pdf

Publications

Contact

Hammerschick, Walter (Administrative Director)
Tel.: +43 1 526151621
E-mail

Subjects

Scientific Research

Information source: SESAM

Last updated on 2015-05-19

Retrieved on 2016-07-20

Permalink: http://cordis.europa.eu/result/rcn/164363_en.html