Report of the

Societal Impact Expert Working Group

EC DG ENTR Report

February 2012

Prepared by Ms. Sadhbh McCarthy, Centre for Irish and European Security

Acknowledgements

The report has benefited from the partcipation and contributions of all members of the expert advisory group. In particular the content of the report has drawn from the written submissions, editorial reviews and comments of Prof. Peter Burgess and Dr. Ben Hayes.

In addition we would also like to thank Dr. Anke van Gorp, Dr. Steve Wright and Mr. Jean Marc Suchier for their valuable wriiten contributions.

This work of the Group and the impact of its output has been facilitated by Ms. Eva Engdahl, DG ENTR.

Table of Contents

01. Introduction

On 1 July 2010 DG Enterprise organized a workshop on Societal Security in R & D. The workshop was framed by a consensus that the Framework 7 Security Research Programme is at a key moment in its life cycle and that the agenda for security research and development in Horizon 2020 is gradually taking shape.

Towards the end of 2010, the Societal Impacts of Security Technology group was set up as a direct outcome of the ESRIF final report. Over the last decade the Global security landscape has altered significantly and across Europe, Member States looked to the security industry to provide new capacities and capabilities to protect European citizens from future threats and incidents, both natural & manmade. However, the securitization of society is a complex process and involves a range of impacts and consequences, some real and some matters of conjecture and perception, all of which need to be addressed. The role of the Societal Impacts Expert Working Group is to bring together experts from the security industry, academia, the NGO and policy communities to ensure we have an adequate understanding of what is being proposed: both the advantages and dis-advantages. The current group has a rich background of knowledge and experience, in their own right, whilst enjoying wider memberships of significant sets of related networks of other technical and legal experts.

Two relevant security principles:

1. *The **security dilemma** states that a perception of disproportionate technical security measures causes unrest and insecurity.*
2. *The principle of **moral hazard** states that the more secure people feel the more recklessly they behave. Thus added security measures without accountability lead to diminishing real security.*

Finally, technology proliferates and security technology proliferates more quickly than most. Clearly, it would be inconsistent for the EU to evolve security innovations, which respect our treaty obligations to civil liberties and human rights, whilst servicing the security regimes of other states that simply do not. The Arab Spring has provided clear insight into dreadful consequences of allowing such double standards to continue, and we will need to consider in the future how each and every security innovation, technology, technique, training and software set should be adequately licensed, regulated and controlled to ensure appropriate consistency and democratic accountability.

02. Rationale & Role of the Societal Impact Expert Working Group

Rationale

The Societal Impacts of Security Technology group was set up towards the end of 2010 as a direct outcome of the ESRIF final report.(footnote to report & reference to societal Security elements of ESRIF) Over the last decade the Global security landscape has altered significantly and across Europe, Member States looked to the security industry to provide new capacities and capabilities to protect European citizens from future attacks.

However, the securitization of society is a complex process and involves a range of impacts and consequences, some real and some matters of conjecture and perception, all of which need to be addressed. Most European Member States remain on high alert and the common personal perception is that we feel much less secure than we did a decade ago. Highly, even over-securitized states have existed before in Europe and our historical experience was that some of them were highly corrosive to human rights, freedom and justice. Today, those values are embedded in our collective legal and treaty obligations, most recently determined in Maastricht, Amsterdam and Lisbon. We remain however vigilant that any advances in security technology should not breach these values or go beyond he limits of the law, whilst ensuring that the best in security innovations can serve o protect all the citizens of the EU without regard to belief, ethnicity or gender.

This is an extremely challenging balancing act since innovation can bring both intended and unintended consequences. The range of technologies is now vast, covering everything from surveillance, biometrics, crowd control technologies, border protection and geo-location and tracking systems, to name but a few.

Role

The role of the Societal Impacts Group is to bring together experts from the security industry, academia, the NGO and policy communities to ensure we have an adequate understanding of what is being proposed: both the advantages and dis-advantages. The current group has a rich background of knowledge and experience, in their own right, whilst enjoying wider memberships of significant sets of related networks of other technical and legal experts.

Name	Organisation
Ms. Sadhbh McCarthy (Chair)	CIES, Ireland
Ms. Eva Engdahl (Co-Chair)	EC DG ENTR
Prof. Peter Burgess	Peace Research Institute Oslo (PRIO), NO
Dr. Ben Hayes	Statewatch International, UK
Dr. Emilio Mordini	CSSC, Italy
Dr. Merle Missoweit	Fraunhofer International, DE
Ms. Heather Griffen-Young	TNO, NL
Dr. Ian Brown	Oxford Internet Institute, DE
Mr. Johann Cas	Austrian Academy of Sciences, Austria
Dr. Anke Van Gorp	University of Applied Sciences,Utrecht, NL
Prof. Bengt Sundelius	FHS, SE
Dr. Steve Wright	Leeds Met. University, UK
Dr. E. Anders Eriksson	FOI, Sweden
Mr. Jean-Marc Suchier	MORPHO (Sagem), FR
Mr. David Wright	Tri-Lateral Research Consulting, UK
Mr. Tim Cooper	Frontex, PL
Mr Henri Delaue	Ind. End User Consultant, FR
Ms. Eleanor Travers	European Civil Aviation Committee, FR
Dr. Gus Hosein	Privacy International, UK
Dr. Joss Wright (Alt.)	Oxford Internet Institute UK
HM Pastuszka (Alt.)	Fraunhofer International, DE
Eric King (Alt.)	Privacy international, UK
Marcel van Belo (Alt.)	TNO, NL
Dr. Holger Mey (Visiting Observer)	*Cassadian , DE*

Table 1. Table of Experts

The collective role of this group is to act as an early warning system for undesirable impacts of proposed technologies and related systems whilst ensuring that the best and most advanced innovations in security systems find adequate support. The challenge is a potent one since research and development in the security sector is well funded with several billion euros already allocated to such work. To ensure this significant resource is appropriately spent, there is a critical need to promote industry but avoid bureaucratic capture. In short, we need to rebalance the mutually dependent requirements of security, freedom and justice.

The Societal Impacts Group has a clear educational function which it is already exercising through the meetings it has held in London, Brussels, Oslo and Warsaw. The group has to wrangle with technologies on the horizon, which may unintentionally bring adverse affects or potentially adverse effects if not accompanied by adequate training, technical standards and democratic accountability. Meeting some of these Social Impact Assessment capabilities with which several members of the group are currently familiar. Other tasks will require new forms of consequence analysis that can be demonstrated to provide the EC with realistic tool boxes to judge future directions in new arenas of security.

03. Approach

Convening of the Group

The most important element of the group is that it is made up of a cross section of participants, representing the broadest possible spectrum of Security Research stakeholders. Initially, the participants were drawn from the nucleus of members of the ESRIF Transverse Committee. The group was augmented by active participants in the July 2010 Societal Security Workshop.

The inaugural meeting was facilitated by the Centre for Irish and European Security (CIES) and hosted by the Oxford Internet Institute (OII).

In addition to the core Expert Working Group, attendees at this meeting also came from the EC agency REA and from the Counter-Terrorist Unit of the UK home office.

All Working Group members have experience with the European Security Research Programme. Most participants have engaged extensively in FP7 projects under the programme. Dr Ben Hayes is the author of the 2009 NEOConOpticon report on the EU Security-Industrial Complex which specifically addresses concerns around the ESRP

The members were selected on the basis of their willingness to assist and participate in the process in a positive and constructive manner.

Process

Over a 12 month period the working methodology was as follows:

- Document Review (existing material & working papers around the subject matter)
- Facilitated Meetings to discuss document input and develop the aspects & approach to Societal Impact and (x4)
- Extended open events to bring the topic to a wider audience and also to solicit comment and input from an extended Stakeholder Group (X2)
- Presentation of the work of the group to Policy workshops and Project Meetings. Following the initial meeting in London,

Ms Eva-Maria Engdahl, DG ENTR, offered the facilitation of the commission, in order to ensure the best possible participation.

MS. Engdahl hosted all subsequent meetings and took over joint chairmanship of the group.

Limitations

Although the T&S costs of the members of the Working Group have been paid by the European Commission, the participation of group members was voluntary and as such the amount of time people had available to work on this was limited.

04. Assesment & Analysis

An initial assessment[1] and the subsequent meetings of the Societal Impacts Expert Working Group have led to the identification of the following concerns:

- Citizen rights;
- Research ethics;
- Societal relevance and
- Security technologies & civil liberties inside & **outside t**he EU

The respect for citizen rights has increasingly been brought into focus as research under the security theme matures. The newly activated Lisbon Treaty gives legal standing to the European Charter of Fundamental Rights, raising questions of both ethical coherence and adherence to the Charter. When citizens' rights have been considered in either project design or the ethical review of projects it has often been considered as an add-on. Citizen rights should however be a fundamental requirement which could and should lead to drawing boundaries of what is and what is not acceptable in EC funded security research.

Research ethics refers to a common set of norms for scientific research in all fields of enquiry. These well-established principles include accountability for scientific procedures, clarification of criteria and choice of research objects, disinterestedness, regard for conflicts of interest, consent of participants in research, confidentiality, transparency of methods and results, respect for data protection and ownership, among other things. There is general consensus that the norms of research ethics are being adequately applied to security R & D in Europe. However, research ethics limits itself to norms concerning the way in which a research project should be performed not with whether there are concerns about the research subject or goals of the research

Societal relevance asks whether research actually leads to enhancing the security of European citizens and how it will affect the lives of citizens in doing so. As self-evident as this question may be it is inadequately thematized, documented and studied in research carried out under the Security Theme. Though few actually disagree that the aim of security research should be to make European society more secure, little reflection is given to how the ambitious technological research carried out under the them can translate, in both positive and negative ways, to societal impact. Two particular themes, resilience and trust where identified as keys for enhancing the effectiveness and standing of the European security research.

---

[1] The assessment of the work done in the first 3 calls of the Security Research Theme was made during the workshop Societal Security in R&D.

Security technologies and civil liberties outside the EU: technology proliferates and security technology proliferates more quickly than most. Clearly, it would be inconsistent for the EU to evolve security innovations, which respect our treaty obligations to civil liberties and human rights, whilst servicing the security regimes of other states that simply do not. The Arab Spring has provided clear insight into dreadful consequences of allowing such double standards to continue. We need to reflect on the necessity and proportionality of security technologies in Democratic society before developing these technologies. Within Technology Assessment methods have been developed that could be used in such an assessment. If the security technology at hand is deemed necessary and proportionate we will need to consider how the security technology, can be adequately licensed, regulated and controlled to ensure appropriate consistency and democratic accountability. This means that even if a security innovation, be it a technology a technique or software is deemed appropriate within democratic societies then we still need to make sure that the innovation is used appropriately in other countries.

How can we address these concerns in the remainder of FP7 and Horizon 2020?

The concerns listed above need to be addressed in different phases of the process from developing the program and call to the actual execution and implementation of research. The Societal Impacts Expert Working Group has identified the following phases:

- Work Programme & Annual calls
- Proposals
- Negotiation
- Project execution
- Implementation of a completed product, system or techniques in different contexts

At the different stages there are different actors and methods to address the concerns. We will go through the phases and present what should be done to address the concerns.

Work Programme/Calls

The question of the societal relevance of European research goes hand in hand with the question of the accountability of public funds. Research that is relevant to the needs of society, which is in tune with the security concerns of citizens, addresses their fears and provides understandable solutions that are regarded as appropriate and proportional will provide an immediate an informal accountability through participation. The need for formal accountability grows out of the impression that resources are being used toward aims that are questionable both in terms of their intention and in terms of their potential for success.

Besides the societal needs, questions regarding the necessity and proportionality of security technologies in democratic societies should be addressed at the call/program stage.

A review of the program and the calls, for example by Security Advisory Group (SEC-AG)[2] is necessary. Important questions that should be answered are:

- Are there any parts of the program of calls that would have to be highlighted from a citizen's rights perspective?
- What evidence is there that the calls ask for projects that have societal relevance? A special case is research that has no direct societal relevance but is aimed at providing policy makers with the evidence base they could use.
- Are the innovations or technologies that are described in the call necessary and proportionate in a democratic society?

Proposals

- Both the proposal review and the ethical review should judge whether the societal relevance of the proposal has been justified adequately.
- During the ethical review the attention is focussed on the proposal itself. The ethical review board has to make a judgment about the following:
- Are the citizen's rights sufficiently addressed in the proposal but also during the research itself?
- Are there provisions in the proposal for the continuous addressing of both the research ethics issues and the subject matter ethics?
- Does the completed technology, system or technique require regulation, control or licensing to ensure appropriate democratic accountability? If so provisions need to be made while the project is running.

Negotiation phase

The project officer should evaluate how the consortium has implemented the recommendations of the ethical review board. It is important that a dialogue is possible. If

[2] There are doubts within the Societal Impacts of Security Technologies expert group whether the Sec-AG is representative enough with regard to societal impact to perform this task.

there is a misunderstanding about the project which leads to requests of the ethical review board that are not practical or relevant there should be a procedure to have a dialogue with the ethical review board. In previous calls there have been examples of misunderstandings leading to requests that could not possibly be met and were also not necessary from, for example, a human rights perspective.[3]

During the project

Put in place a Work Package dedicated to the study of the ethical and societal aspects (the titles vary from project to project).

Have an "independent " team in charge of this WP., but the term "independent does need to be too demanding (it can be different parts of an organisation having different roles within the project. The main issue is that the people in charge of the Work Package and must have some experience in the domain, and must not be involved in the technical Work Packages where solutions are being developed.

The Work Package should cover at a minimum 3 main tasks:

- An initial Societal Impact review (typically during the first 6 months of project). It should cover an analysis of the legal requirements, and known acceptability issues, in the countries of origin of the consortium members, and at EU level, for the topics covered by the project. This would provide initial guidance and information for the developers

- Analysis of the requirements or scenarios defined by the project (after the specification phase), from the Societal Impact and acceptability perspective in order to provide guidance & recommendations for the developers. This is the most important but also the most difficult part of the Work Package. This is where the "societal can influence and improve the results of the project (from the Societal Impact perspective),

- A final Societal Impact Review (end of project). It should summarise the SI issues that have been raised and how they have been handled by the project. It should also mentions what are the potential Societal Impact issues facing the deployment of the solution, and make recommendations on how they should be addressed

[3] One example is that the ethical review board sometimes requests that already in the proposal permission or advice from the data protection authorities of countries where data collection will take place is obtained. It is however not possible to get such permission or advise at that stage from every data protection authority. In the Netherlands for example the College Bescherming Persoonsgegevens (CBP) will not give advice in advance. Moreover, the CBP only needs to give permission if data is gathered about criminal records and health. Data collection on other subjects needs to be registered.

An important issue is that the project coordinator must "believe" in the value of looking at Societal Impact issues. For the IPs, during the hearing phase, this could be possibly looked at through a specific question.

Implementation of a completed product, system or techniques in different contexts

If the societal impacts have been adequately addressed in all previous steps then the solutions that are developed should meet the demands with respect to citizens' rights, societal need and necessity and proportionality in democratic societies. With regard to use and export, states could use a technology in a very different way then what it was developed for. The solutions could be further developed by a user in a way that does not meet the citizen's rights requirements or the necessity and proportionality requirements. Consortium partners and the EC together should make sure that adequate regulation, control and licensing is available for the developed system, technology or technique before it is finished and can be sold or exported.

05. Findings & Recommendations

Findings

- The current ethical review structure in place under the FP7 research protocol focuses on a narrow range of specific issues, and not the wider societal issues that tend to arise in security projects.
- The concept of a broader Societal Impact is insufficiently well articulated within the current ESRP Work Programme (Calls for Proposals or Guidelines for Evaluators);
- The perspective of civil society is not fully represented throughout the ESRP process (e.g., Security-Advisory Group, Programme Committee, Evaluators);
- The results of previously funded projects in this area, for example PRISE, have not been effectively exploited.
- Initiatives based on privacy enhancing technologies and data protection are useful, but cannot replace the wider consideration of ethical issues and human rights.
- The societal impacts of a project are inherently multidimensional, and cannot effectively be assessed through simple YES/NO questions. Any such set of Societal Impact criteria must be sufficiently nuanced to allow for context;

Recommendations

- Societal impact assessment must start at the programme level, and must also be addressed in the work programme topic and text;
- Security research is inseparable from its societal impact. As such, there should be formal consideration of societal impact, up to the level of a dedicated work package for particularly sensitive topics.
- Engage assistance from civil society experts to review the Work Programme as it is being developed.
- For areas or topics that can reasonably be expected to result in significant societal consequences, clear indication of this should be included in the topic description.
- Civil society experts should be formally involved in reviewing the work programme during its development.

- Where areas or topics are considered 'sensitive' to Societal Security issues clear indication of this should be included in the topic description in the work programme and a requirement for inclusion of societal impact clearly stated in the call text.

- Within the work programme a clear narrative of the importance for projects to be in full compliance with the legal and regulatory frameworks, not just in terms of a research project but with the expectation of implementation at some future date in varying contexts.

- DG ENTR, as part of its remit to ensure compliance with ECFHR and data protection legislation, to undertake immediate education and training activities with the technical development teams of current and future projects in relation to the challenges of developing technologies with potentially negative societal consequences.

- REA and DG ENTR project officers with responsibility for security projects to undergo education and awareness training in relation to the societal impact of security technologies and processes.

- Further work should be undertaken towards developing a toolkit for societal impact assessment. In the short-term, a set of high-level criteria should be stated for use in consideration of societal impacts in ESRP work programmes and projects.

06. Societal impact checklist for security R&D

Security is one of many societal values in Europe, all of which must be balanced against one another. Security is a tool in support of freedom that can only be achieved within the rule of law. All EU Member States must abide by both the European Convention on Human Rights and the EU's Charter of Fundamental Rights. The EU and its Member States are in other words bound by law to respect and to promote human dignity, freedom, democracy, equality, the rule of law and protection of fundamental rights, including the right to privacy and data protection, freedom of expression and association, good governance and security.

In support of this obligation, the following questions should be considered as part of Section 3 ('Impact') of the proposal:

Ensuring security research meets the needs of society

1. What documented[4] 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?

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

4. How is the proposed research appropriate to address these threats?

Ensuring security research benefits society

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

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

7. Are there other societal values in Europe that are enhanced by the proposed research?

Ensuring security research does not have negative impacts on society

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

9. If implemented, how could the research impact disproportionately upon specific groups or unduly discriminate against them?[5]

---

[4] (E.g. scientific evidence, social surveys, public perceptions etc.)

10. What specific measures will be taken to ensure that the research outcomes comply with the European Charter of Fundamental Rights and to mitigate against any of the negative impacts described above?[6]

[5] European legislation prohibits discrimination based on grounds such as sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation.

[6] Charter of Fundamental Rights of the European Union, Official Journal of the European Union (2000/C 364/01).