

SecurePART Project

Objective FP7- SEC-2013.7.3.1

Support Action

Increasing the engagement of civil society in security research

Project Number: 608039

D6.6 Production and distribution of press releases & other publications



SecurePART

Increasing the Engagement of
Civil Society in Security Research



1. Change Control

Document Properties

Deliverable No.		D6.6	
Work Package No	WP6	Work Package Title	Dissemination
Author/s		Georgios Kolliarakis (GUF), Jean Cornier (VDL), Elizabeth Isaacs (BANTEC), Maider Goñi (BANTEC), Caroline Davey (SAL), Frank Balzer (NEXUS), Christoph Henseler (NEXUS), Denisa Ionescu (ENNA), Alexandre Almeida (LOBA)	
Reviewer		Alexandre Almeida (LOBA)	
Name		Production and distribution of press releases & other publications	
Date		April 2016	
Dissemination Level		PU	

Revision History

Version	Date	Comments
0.1	1 April 2016	Systematization of all categories of publications and releases (GUF)
0.2	25 April 2016	Integrated draft (GUF)
0.3	27 April 2015	Reviewed by LOBA
1.0	28 April 2016	Final draft (GUF)

This document has been produced in the context of the SecurePART Project. The research leading to these results has received funding from the European Community's Seventh Framework Programme under Grant Agreement SEC-2013-608039.

All information in this document is provided "as is" and no guarantee or warranty is given that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability. For the avoidance of all doubts, the European Commission has no liability in respect of this document, which is merely representing the authors view.



2. Contents

1. Change Control.....	2
Document Properties.....	2
Revision History	2
2. Contents	3
3. Abstract	4
4. CSO guides about communication about and participation in EU research	4
5. Series of Policy Briefs (online & print)	5
6. SecurePART-relevant academic and journalistic publications (online & print).....	6
7. SecurePART Blog	6
8. Press releases about final conference at the European Economic and Social Committee	6
9. The SecurePART Action Plan (online & print)	7
10. The SecurePART Video	14



3. Abstract

This report provides the documentation of all produced, distributed, or published policy briefs, guides, and academic papers in the course of the project SecurePART. It comprises both online and print material, such as guides with SecurePART results, the project's final Action Plan, a series of Policy Briefs about success stories of CSOs in security research, academic and journalistic publications, and press releases about important SecurePART activities.

4. CSO guides about communication about and participation in EU research

4.1 PROJECT FLYER (online & print)

Download: http://www.securepart.eu/download/securepart_flyer_v1150401111304.pdf

4.2 PROJECT FLYER FOR CSOS (online & print)

Download: http://www.securepart.eu/download/flyer_csos150401111234.pdf

4.3 GUIDE FOR PROMOTERS OF COMMUNICATION ACTIVITIES IN THE FIELD OF SECURITY RESEARCH: A SPECIAL FOCUS ON CSOs (online & print)

The aim of this guide is to provide practical information, tips and good practice to security research communication promoters in order to facilitate their activities in the field of security research.

Download: http://www.securepart.eu/download/guidepromoters_140920215150922174556.pdf

4.4 WHY AND HOW TO PARTICIPATE IN HORIZON 2020 SECURITY RESEARCH (online & print)

The objective of this guide is to increase the level of interest and, in the end, the engagement of Civil Society Organizations in Security Research.

Download: http://www.securepart.eu/imagen/guideH2020_30112015.pdf

- Full version in English
- Sumário em Português
- Deutsche Zusammenfassung
- Resumen en Español
- Resumen en Italiano
- Summary in English
- Résumé en Français



4.5 SecurePART FIRST PERIOD RESULTS (online & print)

Brochure with infographs about interim outputs and achieved impacts out of SecurePART activities in the 1st project period.

Download:

http://www.securepart.eu/download/firstperiodresults_04092015150922165650.pdf

5. Series of Policy Briefs (online & print)

In a series of Policy Briefs, SecurePART addressed key dimensions of CSO participation in EU Security Research (Briefs 1-2), as well as conducted studies about the conditions behind 'success stories' and 'best practices' of concrete CSO participation cases (Briefs 3-12):

POLICY BRIEF #1 - State-of-the-art Civil Society Organization (CSO) participation in the European Security Research Programme

http://www.securepart.eu/download/securepart_pb-1160119150839.pdf

POLICY BRIEF #2 - "Acceptance" and "Acceptability" of security-related technologies

http://www.securepart.eu/download/securepart_pb-2160119151110.pdf

Policy Brief #3: CSOs IN SECURITY RESEARCH - Global Risk Forum Davos

http://www.securepart.eu/download/securepart_pb-3160201165737.pdf

POLICY BRIEF #4: CSOS IN SECURITY RESEARCH - Johanniter-Unfall-Hilfe e.V.

http://www.securepart.eu/download/securepart_pb-4160121150517.pdf

POLICY BRIEF #5: CSOS IN SECURITY RESEARCH - Law and Internet Foundation

http://www.securepart.eu/download/securepart_pb-5160122155321.pdf

POLICY BRIEF #6: CSOS IN SECURITY RESEARCH - Stephen Lawrence Charitable Trust

http://www.securepart.eu/download/securepart_pb-6160307150310.pdf

POLICY BRIEF #7: CSOS IN SECURITY RESEARCH - Magen David Adom

http://www.securepart.eu/download/securepart_pb-6160307150310.pdf

POLICY BRIEF #8: CSOS IN SECURITY RESEARCH - The European Forum for Urban Security (EFUS)

This Policy Brief is waiting for approval from EFUS and will be available after the end of the project.

POLICY BRIEF #9: CSOs IN SECURITY RESEARCH - Institute for Strategic Dialogue

www.securepart.eu/download/securepart_pb-9160307121106.pdf

**POLICY BRIEF #10: CSOs IN SECURITY RESEARCH - Austrian Red Cross**

http://www.securepart.eu/download/securepart_pb-10160224091249.pdf

POLICY BRIEF #11: CSOs IN SECURITY RESEARCH – Statewatch

http://www.securepart.eu/download/securepart_pb-11160426120434.pdf

POLICY BRIEF #12: CSOs IN SECURITY RESEARCH - The International La Strada Association

http://www.securepart.eu/download/securepart_pb-12160426120447.pdf

6. SecurePART-relevant academic and journalistic publications (online & print)

Balzer, F.; Henseler, C. (2016): Civil Society Organisation (CSO) participation in the European Security Research Programme. In: Magdeburger Journal für Sicherheitsforschung.

Kolliarakis, G. (2016). From Window-dressing to Windows of Opportunity: Civil Society Actors in the EU Security Regime. In: Marchetti, R. (Ed.) Partnerships in International Policy-Making. Palgrave Macmillan.

Kolliarakis, G. (2016). In Quest of Reflexivity: Towards an Anticipatory Governance Regime for Security. In: Burgess, P. et al. (Eds.): Discourses of Privacy and Security. Routledge.

Kolliarakis, G. (2015). Politics, security technologies, and civil society: the missing links. In: Open Democracy, 29 October 2015.
<https://www.opendemocracy.net/wfd/georgios-kolliarakis/politics-security-technologies-and-civil-society-missing-links>

Kolliarakis, G. (2014). Of Wolves and Sheep: CSO Participation as a Responsible Research and Innovation Mechanism in European Security Research. In: Brodersen, S. et al. (Eds): An Innovative Civil Society: Impact through Co-creation and Participation. Copenhagen.

7. SecurePART Blog

<http://blog.securepart.eu/>

8. Press releases about final conference at the European Economic and Social Committee

Besides the tradition communication by announcing on the website and newsletter, the event was announced at the CORDIS WIRE (RCN: 145316)

http://cordis.europa.eu/event/rcn/145316_en.html



9. The SecurePART Action Plan (online & print)

Launched at the final SecurePART event at the European Economic and Social Committee in Brussels, on 3 March 2016, the Action Plan contains recommendations targeted to each of the identified key stakeholder groups in European Security research, and it refers to actions at the stages of the research cycle which can make a mutually beneficial difference.

http://www.securepart.eu/download/securepart_actionplan160405150624.pdf



Executive Summary

SecurePART Action Plan

for strengthening the links between Civil Society Organizations and Security Research

EC Research Policies on the Science-Society Interface

SecurePART (Increasing the engagement of civil society in security research) is a project which explored ways to strengthen the participation of civil society organisations (CSOs) within the European Security Research programme. SecurePART was funded by EU Security Research Programme, but it also has direct links to two other domains within the EU research Framework Programme: “Europe in a changing world - Inclusive, innovative and reflective societies”; and the cross-cutting research area “Science with and for Society”.

The Horizon 2020 Societal Challenge “Secure societies – Protecting freedom and security of Europe and its citizens” currently involves research in four broad areas: Crisis management and resilience against disasters; organised crime; counter-terrorism, and anti-radicalisation; border control and management; and cybersecurity. Most crucially, security research can be taken to be a proactive form of security policy, creating a pool of potential measures and solutions to address current and future challenges in the increasingly important and contentious policy field of public security.

Enhancing inclusion, legitimacy, accountability, and trust are essential for effective and socially acceptable security research. Highly promising technologies with security-relevant application, such



D6.6 Production and distribution of press releases & other publications

as telecommunication data mining technologies, profiling and predictive analytics, biometric identification and pattern recognition, location tracking technologies, as well as surveillance technologies in the form of drones and CCTV can prove beneficial for the protection of citizens and help prevent major attacks and crises. At the same time, the probability that unsolicited, intentional, or non-intentional misuse of such technologies could generate harm—instead of good—has to be seriously considered.

Many of the outputs from the European Security Research Programme (ESRP) have experienced difficulties in finding their way into effective, legally and ethically compliant deployment. This is due in part to their lack of alignment with practitioners' requirements and needs. 'End users' are practitioners from public, private, or third sector who actually use a product or service; a considerable number among them are civil society organisations (CSOs). The low acceptance of security technologies by citizens worried about the impact on wider society also plays an important role for the limited uptake. Some CSOs focus on privacy and ethical issues, and understand the concerns raised by security research and technologies

The European Security Research Programme (ESRP) has been set up since the mid-2000s under the strong influence of industry, pursuing a predominantly high-tech approach to security challenges, and continues to be dominated by certain stakeholder groups—industry, SMEs, and research and technology organisations. The continued underrepresentation of CSOs limits the potential for the ESRP to successfully respond to emerging security challenges and concerns of European citizens.

Strengthening the engagement of CSOs could help 'ground' security research within real-world societal contexts of application. It might result in security solutions that are more attentive to the expectations and requirements of practitioners. Ultimately, CSO participation could facilitate successful uptake of research results by security providers. CSO participation is not viewed within SecurePART as merely an end in itself, but rather as a means to improve the quality and impact of the research.

Awareness-raising among CSOs can only be considered as the first step in order to overcome institutional and organisational barriers, and help open windows of opportunity for meaningful CSO participation. CSO empowerment will require change by all stakeholders' and at each stage of the ESRP policy cycle. The engagement of CSOs involves them being considered as key stakeholders and ultimately partners at various stages of the ESRP cycle—from evaluation and assessment to agenda setting, and from research implementation, to result exploitation. CSOs can contribute to three core requirements if security research is to unfold a positive impact: (1) ensuring that security research addresses documented needs of society; (2) ensuring that security research benefits society as a whole; and (3) ensuring that security research does not have negative non-intended consequences on society.

A series of EU policies call for a wider, stronger, and more meaningful engagement of citizens and the organised civil society, in order to make policy, including research policy and publicly funded research more responsive to their needs and concerns, as well as more legitimate, and, consequently, also more effective and accepted. These include the EU Lisbon Treaty (including the



D6.6 Production and distribution of press releases & other publications

articles about the mandatory dialogue with the Civil Society, and the article about the Precautionary Principle), the Charter of Fundamental Rights of the EU, as well as the EC policy calling for Responsible Research and Innovation.

At this point, it is worth remarking that ‘participationism’ has become for many public organisations a kind of panacea in order to amend legitimacy gaps, and enhance acceptance of policies. However, CSOs regularly suffer from participation fatigue, realising that their engagement often results in no substantial influence, and their presence gets instrumentalised, by becoming a ‘fig leaf’, or a tick-box exercise for public administration.

The potential to turn the organised civil society from passive addressee and object of research into an active agent and influencer of research and its diverse applications is still largely untapped. European Security Research has been so far, largely “*about*” society, but neither manifestly “*for*” society, nor operating “*with*” society. The time is ripe for taking action in order to change that.

SecurePART Approach & Findings

In SecurePART we pursued a multi-stakeholder governance approach with regard to the ESRP. Besides CSOs from a variety of sectors and regions, with different degrees of familiarity with security research, we explored the views and actions of other research actors from academia, industry and SMEs, but also policy makers from member states, representatives from National Contact Points for EU research, officers from the European Commission with relevant dossiers, as well as officers from the Research Executive Agency. We have scoped other research fields such as genetic technology or nano-technology which have generated controversies in society for stakeholder engagement practices.

After analysing the institutional context of relevant research and engagement policies, we applied a supply-demand (“push-pull”) logic in order to find out about existing, missing or untapped opportunity structures for CSO engagement in the ESRP, but also about capacities and incentives for CSOs and other research actors to come together in a productive manner. This led us to conduct a feasibility/desirability check of all involved stakeholders in order to identify barriers arising from their capacity and willingness to engage CSOs.

In a series of literature and policy document reviews, interviews, online surveys, case studies, workshops and conference panels, we have isolated a number of key findings, which are highlighted in brief here:

Definition and categories of CSOs

According to the European Commission, civil society encompasses trade unions and employers’ organisations (“social partners”), non-governmental organisations, professional associations, charities, grass-roots organisations, and organisations that involve citizens in local and municipal life, including churches and religious communities. These are supposed to lend a voice to the needs of all citizens, and provide a communication channel for them to policy makers. Civil Society Organisations are broadly defined as:

“... all non-state, not-for-profit structures, non-partisan and nonviolent, through which people organise to pursue shared objectives and ideals, whether political, cultural, social or



D6.6 Production and distribution of press releases & other publications

economic." (European Commission (2012), *The Roots of Democracy and Sustainable Development. Europe's Engagement with Civil Society in External Relations*, Brussels, 12/9/2012. COM(2012) 492 final)

A preliminary analysis of the CORDIS database conducted by SecurePART helped discern the following categories of CSOs, many of which are practitioners of security provision:

- Medical disaster first aid/relief associations;
- Emergency Services (Fire brigades & rescue services);
- Transport associations & passenger rights NGOs;
- Community & neighbourhood integration associations;
- Human/civil rights associations;
- ICT/cyber liberties & data protection organisations;
- Climate change and environmental organizations;
- Development cooperation organizations;
- Think Tanks & foundations;
- Science dissemination organisations

Many of the above categories contain hybrid organisations, which are on the border between public administration, research organisations, or small enterprises. Yet a major challenge is the lack of a clear, jointly shared and legally binding definition of what is a CSO.

CSOs are under-represented within EU security research projects. The SecurePART coding in the CORDIS database resulted in an approximate percentage of 4% of CSOs out of ca. 2,000 total beneficiaries. However, the ex-post evaluation of FP7 Security theme (2015) did not differentiate among CSOs and other organisations, and CSOs necessarily fell into the category "Other", accounting for around 3% of total participations.

Barriers to CSO participation in Security Research

In a series of interviews, online surveys, and an interactive CSO-Stakeholder workshop, SecurePART found out that:

There are CSOs that appear to have an explicit interest in security research and have participated/can participate in research actions. However, more than one third of the interviewed CSOs do not readily recognize much relevance of security research to their activities—at least not at first sight—and therefore do not participate. There is also a considerable proportion among the interviewed CSOs which have an explicit interest in security research, but lack access to research actions. This highlights target groups of CSOs for security research offering an untapped potential. Those that do not yet recognise the relevance of SR could be sensitized and mobilized to participate in future research actions for mutual benefit; Those already willing to participate need better access opportunities.

CSO representatives, from a diverse range of backgrounds, stated that their motivation to participate in EU security research is linked with their activities on the ground, also linked to political, social, and ethical concerns of the citizens.

In general, CSOs are confronted with a series of internal and external barriers when it comes to the European Security Research Programme. CSOs face the challenge of being informed and being visible to other security research actors, link their organisation's mandates with the concrete security research topics, and, not least, employ the appropriate staff to conduct research. What is more, many CSOs seem to be alienated by the predominantly



D6.6 Production and distribution of press releases & other publications

technological focus of the ESRP, as well as deterred by administrative hurdles, and by the poor relationships with other security research actors. Unfortunately, there is a lack of CSO networks in security-relevant fields to promote their agendas at EU level.

At the same time, it is not easy for research administrators at the European Commission to recognise advantages and benefits of CSO engagement in security research actions. The situation may be exacerbated by a tendency amongst project co-ordinators and partners (such as research and technology organisations, universities, or industry including SMEs) to not include CSOs in their activities, or simply assign them dissemination roles or less-substantial tasks.

A frequent point of resistance toward wide (CSO) participation from the side of industrial developers and commercial service providers is confidentiality about security research outputs fearing about patents and comparative market advantages.

Roles for CSOs in security research

CSOs have already undertaken a number of roles within security research with different intensity in terms of format, and different goals, while they still aspire to undertake roles with more influence:

1. *Observers*: CSOs get information on H2020 programme at info days, project and policy conferences;
2. *Advisors*: CSOs are invited to become members in external advisory boards during the project implementation phase;
3. *Actors of research*: CSOs participate in research as members of a project consortium, often as disseminators raising awareness to key target groups;
4. *Project evaluators & reviewers*: CSOs are invited by the EC services as external experts to conduct evaluations and reviews;
5. *SR agenda consultants*: CSOs are consulted during the drafting of the future SR programme agenda;
6. *Commissioners of research*: CSOs formulate research calls with a strong SR relevance

Those roles, are usually played at a stage or throughout the policy cycle of security research, which can be for analytical reasons depicted as such:

Recommendations to SR Stakeholders

To CSOs

- ➔ Get informed about the four areas of security research and identify possible common ground with your activities. Consider the potential benefits of participation opportunity to fulfil own goals as well as spread good practice further afield



D6.6 Production and distribution of press releases & other publications

- Use online and live consultations to give feedback to the European security agenda about concerns and aspects from your work on the ground (*stage I, II*)
- Organise with regard to security-relevant research by forming or becoming members of European advocacy networks which can interact with the European institutions and communicate your interests (*stage I, II*)
- As a project partner, ensure that you are not merely a passive distributor of results, or an advisor, but you get the chance to exercise an a) early, and b) strong influence on the research questions too (*stage III*)
- Build up your reputation as a competent and reliable project partner by professionalizing your research structures, and by employing the appropriate staff (*stage III*)
- Provide a “reality check” to security research: Since you are in direct contact with citizens or other CSOs, you are best equipped to point to potential non-intended negative consequences of research, but also act as a translator and multiplier in order to enhance their positive impact (*stage IV, V*)

To potential Coordinators (RTOs, SMEs, Universities)

- As potential coordinators of SR actions you are important facilitators for CSO participation. If you invite CSOs to join early on in the proposal formulation process, and give them a substantial role in the consortium, you may increase the robustness and usability of the project’s results (*stage III*)
- Make sure that you reach out to civil society actors (either in your external expert board, or in your workshops and events) throughout the project for feedback and critique, in order to reflect on potential benefits and costs of your recommendations for the third sector in society (*stage III*)
- CSOs can help to pave the way for innovations in society. Involving them in the application and implementation phase of projects can



D6.6 Production and distribution of press releases & other publications

contribute to enhancing acceptability and acceptance of your research (*stage IV*)

To National Contact Points

- Inform and sensitize the delegate of your MS in the “Secure Societies” Programme Committee about the potential of CSOs as beneficiaries and as ‘end-users’ in the ESRP with particular interests and strengths (*stage I, II*)
- Act as matchmaking hubs by using detailed registers of CSOs and their specific areas of activities in order to bring the right CSOs in contact with relevant calls and applicants’ consortiums (*stage III*)
- Raise awareness among CSOs about the ESRP, and facilitate their participation e.g. at general and dedicated Info-days about the ESRP calls (*stage III*)

To the European Commission /REA

- (EC) Reach out to existing CSO networks, and, additionally, include CSOs in a dedicated Mobilisation and Mutual Learning (MML) platform, in order to create awareness of emerging challenges in the security research field, valorise existing results for security practitioners, and, not least, foster mutual commitment for the future security research programme (*stage I, II, IV*)
- (EC) Treat CSOs as a distinct interest/stakeholder/expert group and invite them to ad hoc and regular consultations. Allow for a wider stakeholder diversity in the “Protection and Security” Advisory Group by accepting more CSOs and gain a better grasp of the dynamics of security technologies in societal context (*stage I, II*)
- (EC) Introduce the instrument of problem-centred (instead of solution-centred) “Open Calls” by earmarking a part of the budget in each annual programme for institutional and organisational issues of security in order to receive bottom-up (unexpected) innovative ideas from the ground and enhance the reflexivity of the ESRP (*stage II*)



- (EC) Explore common denominators and issue joint calls by bringing together the research areas of “Secure Societies”, “Inclusive, innovative and reflective societies”, as well as the cross-cutting research area “Science with and for Society”. This will help to better connect technological with non-technological aspects of security.
- (EC) Promote particularly in the context of pilot/demonstration projects mandatory participation of CSOs as key innovation facilitators, since they are best sensors of the societal context and its enabling/constraining conditions for effectiveness, legitimacy, and acceptability of new security provision mechanisms (*stage III, IV*)
- (REA) Support CSOs by assisting with administrative hurdles, in order to foster equal participation chances also to small CSOs as project beneficiaries, which have a solid knowledge of security issues on the ground, but little experience in research (*stage III*)
- (REA) In terms of evaluation and review of projects, engage more CSOs with practical experience as experts for the sake of a “reality check” in practice, and penalise one-sided participation in consortiums which neglect the third sector (*stage V*)
- (EC & REA) Conclude on a joint CSO operational definition and start differentiating among CSO beneficiaries in the internal statistics (CORDA, SESAM) with regard to their participation modalities and their impact on the overall success of the project (*stage V*)
- (EC & REA) Establish success criteria and innovation indicators beyond financial auditing which better capture positive impacts beyond marketing, and Communicate about success stories with CSO-involving projects (*stage IV, V*)

10. The SecurePART Video

SecurePART Video was uploaded to the website and youtube and published at the CORDIS twitter and youtube accounts.

<https://www.youtube.com/watch?v=YVGPObEluK8>

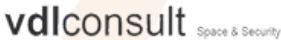


Contract No. FP7- 608039 SecurePART is a project co-funded by the European Commission under the Seventh Framework Programme

www.securepart.eu



www.bantec.es



www.vdlconsult.de



www.ennaurope.org



Institut für Kooperationsmanagement und interdisziplinäre Forschung

www.nexusinstitut.de



www.uni-frankfurt.de



www.salford.ac.uk



www.loba.pt