SECUREPART ACTION PLAN FOR STRENGTHENING THE LINKS BETWEEN CIVIL SOCIETY ORGANIZATIONS AND SECURITY RESEARCH
EXECUTIVE SUMMARY

www.securepart.eu
1. 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 under the EU FP7 ‘Security Theme’, but it also has direct links to two other domains within the current EU Research Programme ‘Horizon 2020’: “Europe in a changing world – Inclusive, innovative and reflective societies”, as well as with 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. Security research can be taken to be a crucial 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, serving the goals of the 2015 European Agenda on Security in a strategic manner.

Enhancing inclusion, legitimacy, accountability, and trust are essential for effective and socially acceptable security (research) policy. Highly promising technologies with security-relevant application, such 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, abuse of such technologies could generate harm—instead of good—has to be seriously considered and already during the research stage averted or minimized.

Many of the outputs from the European Security Research Programme (ESRP) have experienced difficulties in finding their way into effective, legally and ethnically compliant deployment by security practitioners. 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, while questioning their effectiveness in practice.

The European Security Research Programme 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 ESPR policy cycle. Engagement of CSO as key stakeholders with invaluable ‘hands-on’ knowledge and capabilities aims at involving them at various stages of the ESPR cycle—from evaluation and assessment to agenda setting, and from research implementation to result exploitation as equitable partners. 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 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 founding document of Horizon 2020 and the EC policy in support of 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, or 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 as a tick-box exercise for public administration, turning them into a ‘fig leaf’ for policies serving other interests than the ‘public good’.

The potential to turn the organised civil society from passive addressee and object of security research into an active agent and influencer of research is still largely untapped, despite the enormous political salience the field of public security has gained in the past couple of years. 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.

2. SecurePART Approach & Findings

In SecurePART we pursued a multi-stakeholder governance approach with regard to the ESPR. 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”) model in order to find out about existing, missing or untapped opportunity structures for CSO engagement in the ESPR, 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, interactive workshops and conference panels, we have isolated a number of key findings, which are highlighted in brief here:
2.1 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 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).

Civil Society Organisations form a diverse but vibrant ecology in the EU member states, and they are actively present also in research. 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 are practitioners in security-relevant fields. They often 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 undifferentiated category “Other”, accounting for around 3% of total participations.

2.2 Barriers to CSO participation in Security Research

In a series of intensive structured exchange with CSOs, SecurePART found out that:

There are CSOs that appear to have an explicit interest in security research and have participated/are willing to 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 lack the overall interest in security research. There is also a considerable proportion among the interviewed CSOs which, despite having explicitly an interest in security research, but lack access to research actions.

This highlights target groups of CSOs offering an untapped potential for future security research planning. Those that do not yet recognize 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 mandated 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 participating in the European Security Research Programme. CSOs face the challenge of being informed and being visible to other security research actors in the first place, 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 technological focus of the ESRP, as well as deterred by administrative hurdles, and by the poor relationships with other, influential security research players, e.g. from the industry.

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 always 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) not to engage CSOs in their activities as equitable partners, or simply assign them dissemination roles or less-substantial tasks, on grounds of their inexperienced with research proper. 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.
2.3 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, and they aspire to undertake roles with more influence. Increasingly more decision makers recognize the need to engage CSOs in order to ground security and research policies into an empirically grounded, evidence-informed base from the context of application:

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 one or more stages, or throughout the policy cycle of security research, which can be for analytical reasons depicted as such:
3. Recommendations to SR Stakeholders

The following recommendations are addressed to key stakeholder groups and correspond to the security research cycle. The evidence which builds their background, along with a series of ‘Success Stories’ and ‘Best Practices’ is documented and further elaborated in the reports published by SecurePART, publicly available under www.securepart.eu.

**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 opportunities in order to fulfill own goals as well as spread good practice further afield.

- **Use online and live consultations to give feedback to the European security (research) agenda about concerns and aspects from your work on the ground** *(stage I, II)*

- **Organise your interests with regard to security–relevant research by forming new or becoming members of existing 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

- As potential coordinators of SR actions you are important facilitators for CSO participation. If you invite CSOs to join early on as partners in the proposal formulation process, and give them a substantial role in the consortium, you may increase the robustness, acceptability, and usability of the project’s results (stage III).

- CSOs can help to pave the way for innovations in society by elucidating the non-technological conditions for innovation diffusion and uptake. Involving them in the application and implementation phase of projects can contribute to enhancing acceptability and acceptance of your research (stage IV).

TO NATIONAL CONTACT POINTS

- Inform and sensitize the delegates of your Member State 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).
(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 within societal context (stage I, II).

(EC) Introduce the instrument of “Open Calls” by earmarking a part of the budget in each annual programme in order to receive bottom-up (unexpected) innovative ideas from the ground and enhance the reflexivity of the ESRP. The calls may take an ‘open contest’ character and invite problem- or solution-centred innovative proposals about institutional and organisational issues of security (stage II).

(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, or limited logistic capacities for 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 in society (stage V).

(ReA) Promote particularly in the context of pilot/demonstration projects mandatory participation of CSOs as key innovation facilitators in project consortiums, 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) Explore common denominators and issue joint calls on specific issues by bringing closer 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 in ‘cross-over’ topics which better simulate application in real circumstances.
- (EC & REA) Elaborate and launch 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 can better capture positive impacts beyond marketing uptake, and communicate success stories with CSO-involving projects (stage IV, V)