SecurePART

Increasing the Engagement of
Civil Society in Security Research

In this Issue...

What is SecurePART?

Started in May 2014, the main goal of the SecurePART project is to contribute to the increased engagement and involvement of civil society organisations in EU-funded security research in order to (i) improve the capacity for social, non-technological innovation; and (ii) address the problem of acceptance of security research outputs by wider society.

In order to do so, we will focus our efforts on achieving our objectives.
SecurePART OBJECTIVES:

OBJECTIVE 1

Understanding the current level of CSO participation in security research;

OBJECTIVE 2

Supporting CSOs in dealing with the increasing complexity of security research;

OBJECTIVE 3

Increasing the structural capacity of CSOs to participate in security research. For example, by promoting collaborative links between CSOs with similar interests, or between CSOs and relevant stakeholders in security research;

OBJECTIVE 4

Defining a strategy and developing an action plan identifying concrete steps to increase CSO participation in both the shaping and the implementation of EU-funded security research.

SecurePART will achieve these objectives through delivering the following tasks:

1.
Investigating the extent to which CSOs have been involved in previous and ongoing EU Framework Programme 7 (FP7) security research projects;

2.
Reviewing other EU-funded research outside the security domain that also experiences problems relating to acceptance by the public;

3.
Reviewing existing Societal & CSO analyses

4.
Developing a communication plan to promote the potential benefits of CSO involvement in security research

5.
Formulating a strategy for increased CSO participation and a well-defined action plan

The work undertaken by the SecurePART project will make a significant contribution to the expected impact of this European security topic. It will provide deeper insight and wider awareness of the European security-related research, industrial landscape, public context and the frameworks in which stakeholders operate.

In particular, actions will indicate opportunities and constraints for developing and strengthening a European security-related market.

Based on an understanding of good practices from other research fields, SecurePART will propose new strategies to better integrate CSOs in the security research in a sustainable way. This will directly and indirectly improve the impact of EU security research by engaging important stakeholders and closing the gap between research and public needs.

Furthermore, by involving CSOs with different remits and agendas, new perspectives and insights will be brought into security research, which have the potential to increase innovation.

SecurePART will strengthen and enlarge the network of organisations involved in the EU security research field, and will establish a new network of research institutes.

www.securepart.eu

Editorial

Welcome to the first newsletter of the SecurePART project. This issue provides an introduction to the project for those who would like to know more about its goals, developments and expected results.

For those already familiar with SecurePART, there are updates on the status of project tasks, news about dissemination activities and short articles on relevant issues.

The project consortium is now contacting representatives of civil society organisations, as well as their collaborators and other stakeholders in security research (academic researchers, industry representatives, policy-makers, consultants and other facilitators). Their input and cooperation are essential to the success of the SecurePART project. **Your feedback is welcome!**

THE SECUREPART PROJECT TEAM

What is a civil society organisation?

Civil society refers to all forms of social action carried out by individuals or groups who are neither connected to, nor managed by, the State. The term civil society organisation applies to all organisational structures whose members serve the general interest through a democratic process, and who take on the role of mediator between public authorities and citizens.

In particular, civil society organisations represent:

- Participants in the labour market, through social partner organisations;

- Specific socio-economic groups;

- Non-governmental organisations which champion common causes (environmental protection, consumer rights, education and training, etc.);

- Grassroots organisations representing a section of society (youth movements, family associations, etc.)

- And religious communities.

The Lisbon Treaty (Article 15 of the Treaty on the Functioning of the European Union-TFEU) recognises the importance of civil society participation to good governance in Europe. Therefore, while the functioning of the European Union is founded on representative democracy, Article 11 of the Treaty on European Union provides for the establishment of an open, transparent and regular dialogue with civil society organisations. When preparing legislative proposals, the Commission consults civil society organisations concerned with Union activities.

Source: European Union Glossary @
http://europa.eu/legislation_summaries/glossary/civil_society_organisation_en.htm

What is security research?

All research and development of technologies and knowledge for building capabilities needed to ensure the security of European citizens from threats such as terrorism, natural disasters and crime, while respecting fundamental human rights including privacy.

What types of organisation are or should be being engaged in EU security research?

Participants in European security research include security industry, technology companies, research organisations and end-user. The European Union aims to broaden participation and better represent the interests of wider society, through the involvement of CSOs.

The types of CSOs relevant to European security research include:

- Community-based and neighbourhood organizations or groups Development and 'Peace' NGO;

- Human rights groups or networks;

- Advocacy organizations or groups (i.e. campaign group, public interest group);

- Lobby groups (pressure group, private & business interest group);

- Network or support groups devoted to societal empowerment;

- Policy research institutes, think tanks or security studies institutes;

- Professional associations or groups;

- Student groups;

- Trade union or employers organizations;

- Academic associations or networks;

- Women's organizations;

- Faith-based organizations;

- Non-operational charitable organizations (i.e. grantmaking foundation);

The Challenge

Security policy and security research are sensitive and contentious public policy fields involving values and principles in knowledge creation and implementation.

Despite their relevance for comprehensive problems faced currently by European societies, deliberation about problem definitions, goals, and methods of security research have been restricted mainly to experts and particular interest groups.

This has led to the dominance of a "high-tech" technology-centred conception of security. There is an urgent need to integrate civil society actors earlier and more intensively into a responsive and responsible policy process, as they are the ultimate beneficiaries and are most affected by research on security technologies.

Public concern is growing about how new security technologies impact on society, such as biometrics, pattern recognition and detection, risk profiling, or the use of surveillance 'drones'. What is at stake with these and other technologies goes far beyond issues of privacy and data protection, posing fundamental questions around the feasibility, legitimacy and desirability of maximum-security societies. If ethics and societal impacts are to be properly addressed in current and future EU security research programmes then comprehensive appraisal by citizens themselves is required.

Stakeholders Board Meeting Presentation

The purpose of the Stakeholders Board Meeting was to provide an opportunity for more intensive interaction between the main consortium members and the project experts group.

It was organised:

A

To obtain feedback on the initial findings of work packages 1 and 2;

B

To seek advice on the selection of the case studies to be conducted;

C

Obtain input in relation to success stories, practices, platforms, networks and other initiatives involving CSOs in security and other fields of research.

The meeting was organised in Strasbourg, in order to take advantage of the World Democracy Forum 2014 held by the Council of Europe 4th November 2014. The meeting adopted a focus group approach in order to structure the exchange between participants, covering three areas:

• The extent to which the experience of FP7 research can inform future civil society–oriented security research;

• The transfer of experience in relation to the improvement of societal acceptance from other technology research areas to security research;

• The structure of the next SecurePART multi–stakeholder workshop to be organised mid–2015.

External participants that attended the meeting were as follows:		
Milos Jovanovic	EvoCS project coordinator	Germany
Hendrik Keersmaekers	Legal Affairs Manager, G4S Belgium	Belgium
Ineke Malsch	S&T societal dialogue specialist, collaborator with a CSO in biosecurity issues, member of the advisory board	The Netherlands
Sadhbh McCarthy	Director of the Centre for Irish and European Security (CIES), member of the advisory board	Ireland
Henk Mulder	Coordinator Science Shop, member of the advisory board	The Netherlands
Hugo Rosemont	Security Analyst and Adviser. Independent social researcher	United Kingdom
Tom Sorell	Professor of Politics and Philosophy, member of the advisory board	United Kingdom

Building on the experience of other technology fields

In Workpackage 2, the objectives of Task 2.1"Technology Field Selection" are to:

1

Select dominant controversial technology fields with exemplary attempts at civil society integration.

2

Collect sufficient reference data for the identification and analysis of good practice examples of civil society integration.

History shows that many new technologies face societal controversies leading even to potential public rejection of their use. The success of an innovation process depends primarily on the public acceptance of the innovation.

Evidence shows that controversial technologies have responded to the challenge by the development of dedicated programs to improve public acceptance. The European security research is a fairly new technology field and, without doubt, a controversial one. Therefore, SecurePART can learn from successful methods and strategies for addressing wider society concerns adopted by other technology

Work package 2 selected six technology fields that answered 'yes' to the following question:

Do public communities in Europe consider the technology field controversial and does this raise issues about societal acceptance?

THESE FIELDS ARE:

Space Technology

Chemical Technology

Nanotechnology

Genetic Engineering

Environmental–Technology

Energy Technology

The six selected technology fields were then reviewed using a number of criteria for their suitability as models of good practice. Three fields displaying complementary characteristics were chosen for more detailed analysis, as follows:

Genetic Engineering
High CSO involvement and societal impact;

Chemical Technology
High European relevance and technology maturity;

Energy Technology
High societal and economic.

Space Technology	Chemical Technology	Nano-technology	Genetic Engineering	Environmental Technology	Energy Technology

Field Selection

3.
For detailed analysis

Figure 1: Technology Field Selection

The next steps to be performed in Task 2.2 – "Analysis and detailed review" will be to examine the approaches to build trust and achieve societal acceptance, and to identify the best initiatives, tools and practices regarding their applicability and feasibility in security technology.

4th World International Studies Committee Conference

European Civil Security: A New Paradigm for Security Research and Policy?
Frankfurt, 6–9 August 2014

In the context of the theme "Security and development, civil and military cooperation: Pitfalls and opportunities" of the 4th triannual conference of the World International Studies Committee (http://www.fb03.uni-frankfurt.de/46347686/wisc), Georgios Kolliarakis invited experienced experts in the European Security Research Programme (ESRP) to discuss the state-of-play and future trends in the policy field of the ESRP. Experts included: Steering Committee members, Security Advisory Group members, representatives of Research and Technology Organisations, and international CSOs.

1.

How to tackle the issue of 'Dual Use', i.e. feasibility and desirability of separating military from civilian applications of security technologies?

2.

How to reconcile the promotion of high-tech innovations with ethical, privacy and equal access concerns of citizens, along the lines of Responsible-Research-and-Innovation policies of the European Research Area?

3.

How to guarantee a balanced participation of stakeholders in defining the agenda, the implementation and monitoring of research projects, in order to make the ESRP more legitimate, and more responsive to the needs of its ultimate beneficiaries-the European citizens?

4.

How to assess and evaluate the outcomes and, most importantly, the financial and social impact, of research and development of security technologies?

Further details about the round table can be found:

http://www.securepart.eu/files/WISC_RoundTable_newsletter.pdf

The panel attracted an audience from around the globe and from a wide range of disciplines. The topic of security research, its potential benefits and implications for society stimulated a lively discussion between experts on the panel and the scholars. In particular, two key questions were raised: who should define the meaning of real "innovation" in relation to society? Who are the stakeholders in security research? The conference proved an opportune time to present the overall agenda of SecurePART to an expert audience and explain the need to make security research more transparent, accountable and accessible to civil security actors.

Council of Europe, World Forum for Democracy,

Young citizens: Unlocking the freedom-versus-security debate
Strasbourg 3–5 November 2014

At the 3rd annual World Forum of Democracy (link: http://www.coe.int/de/web/world-forum-democracy), organised by the Council of Europe in Strasbourg, more than 1000 participants from the 47 member states plus associated countries convened to discuss how young citizens should engage in shaping future democracies.

SecurePART was invited to address the question of how much freedom young citizens are prepared to give up in order to be secure. Formulated in Thomas Hobbes' Leviathan in 1651, this challenge been recently rekindled by the rise of the internet and other information and communication technologies. Freedom of expression, right to information, connecting socially with people far away, are evolving in liberal democracies together with

security risks, such as abuse of the private sphere, mass surveillance, discrimination of minorities, and even violence. Young citizens in particular, socialised in the era of social media, should reflect on the costs and benefits of online communication, and seek out opportunities for responsible action to shape open and secure democratic societies of the future.

The online communication world has long become the public sphere of the 21st century: The internet, navigated by PCs, tablets, and mobile phones, is increasingly turning for more and more citizens into a free association forum, a marketplace, or an education site, where exchange of ideas and the building of social relationships enters a novel dimension. The vast

spectrum of possibilities opened up by new technologies for engaging and participating in genuine democratic procedures nonetheless has a downside. The Cloud, Big Data, and geographic positioning identification technologies, developed and used for that purpose, may be abused by criminal actors, by private companies pursuing their own commercial interests, or even by states in order to monitor and control citizens' activities–both within their national territory and worldwide.

The discussion, organised in three world–café groups, identified the main concerns of the participants and explored courses of action to make the Internet an open and secure public space for exchange in the 21st century.

THE THREE CORE CHALLENGES THAT WERE CONSIDERED WERE:

1.

How do young citizens perceive fun, freedom, new possibilities, but also constraints and threats to their liberties and rights in the social media?

Are there limits to online communication in social networks and, if so, who should set them?

2.

Where does responsibility for safeguarding freedom and providing security in the internet lie? Does it lie with states, international organisations, businesses, technology developers, non–governmental organisations or with civil society?

3.

Where and how should young citizens become sensitised and actively involved in order to increase their influence and leverage at co–shaping the future of online democracies? Should this be primarily through law–making, by increasing their awareness and cyber–literacy or through online activism?

Download the flyer of the unconference

http://www.securepart.eu/files/flyer_preview.pdf

More and more citizens, particularly the young, are full-time netizens. Recent revelations, such as those initiated by Edward Snowden in 2013, have pointed to illicit mass surveillance of everyday behaviour under the pretext of guaranteeing public security. How new information and communication technologies (ICT) are developed and applied within a democratic context is affected by the extent to which the new generation is able to realise their rights in the 21st century.

SIS-RRI Conference in Rome

19th to 21st November 2014

In the context of the Italian Presidency of the Council of the European Union, the European Commission co-organised a high-level conference on Science, Innovation and Society: Achieving Responsible Research and Innovation (SIS-RRI) (http://www.sis-rri-conference.eu/programme/view-full-programme/), November 2014 in Rome.

The main aim of the conference was to define an effective instrumenfiret for the European Commission in order to plan future RRI framework actions and objectives.

THESE SHOULD FOCUS ON:

A

"Prompting new governance strategies for science and scientific institutions"

B

"Fostering Research Integrity in Europe"

C

"Defining new tools for understanding society"

Forecasting changes and ameliorating the exchange between science and society. Public engagement and the integration of civil society in the governance process of research are two of the main pillars of RRI and are explicitly addressed by SecurePART.

SecurePART explores how to foster engagement of civil society actors, who are the ultimate beneficiaries of research on security technologies, throughout the policy cycle of security research, in order to enhance both its legitimacy and its effectiveness. A poster from the SecurePART project about **The Societal Impact of Security Technologies: Making European Security Research more Responsive and Responsible** has showcased three potential governance mechanisms.

THE POTENTIAL GOVERNANCE MECHANISMS ARE:

1.

Upstream and streamline CSO participation, particularly in the problem-formulation and agenda-setting stages of security research

2.

Reflect upon the high-tech biased notion of innovation, which results in a rather naïve technological solutionism

3.

Introduce societal impact assessments, in order to assess the desirable but also the unintended and unanticipated consequences of security technology development at an early stage to avoid an adverse public reaction.

These should contribute at different stages of the security research policy cycle to making both the process more accountable and responsive to the citizens' needs, and to making the results more socially and ethically acceptable.

The SIS-RRI conference conveners have drafted the **"Rome Declaration"** (http://www.sis-rri-conference.eu/wp-content/uploads/2014/07/RomeDeclaration.pdf). This document which lists a series of future-oriented recommendations to be discussed in the Council of the EU Ministers responsible for Research policy in December 2014. Increasing and strengthening the participation of civil society in research has not only been a central focus of the panels and roundtables at the conference, but it is also explicitly stressed in the text of the Rome Declaration. SecurePART, funded under the Security Area of FP7, is one of the very few projects outside the "Science-in-Society" area to directly address those aspects with regard to security research.

Presentation of the web survey

Public concern is growing about a range of new security technologies such as biometric IDs, risk profiling and the use of surveillance 'drones'. What is at stake with these and other technologies goes far beyond privacy and data protection to core questions around the feasibility, legitimacy and desirability of maximum security societies.

We understand that security research comprises development of new technologies and knowledge for building capabilities needed to ensure the security of citizens from threats such as terrorism, natural disasters and crime, while respecting fundamental human rights including privacy and irrespective of their inclusion in the priorities of the specific FP7 Security theme.

If at any time during the last 6 years you have been a collaborator and/or staff of a CSO, your point of view is welcomed within this survey, even if you are not familiar with the issues of security and research.

Please, fill in the survey at
www.securepart.eu/survey

Project Website

Nowadays, a website is one of the primary, if not the main, media for the dissemination of project activities and achievements. As a consequence, the design and setup of the SecurePART website has been one of the first tasks after the project's kick-off meeting .

To keep in touch with SecurePART, please visit the website at:
http://www.securepart.eu.

Partners

BANTEC GROUP
www.bantec.es
lb@bantec.es

VDLCONSULT
www.vdlconsult.de
j.cornier@arcor.de
lippe@vdlconsult.de

ENNA
www.ennaeurope.org
denisa.ionescu@ennaeurope.org

NEXUS INSTITUTE
www.nexusinstitut.de
henseler@nexusinstitut.de

GOETHE UNIVERSITY FRANKFURT
www.uni-frankfurt.de
kolliarakis@soz.uni-frankfurt.de

University of Salford United Kingdom
www.salford.ac.uk
c.davey@salford.ac.uk

LOBA *(GLOBAZ, SA)*
www.loba.pt
alexandre@loba.pt

SecurePART
Increasing the Engagement of
Civil Society in Security Research