DPT

Deutscher Präventionstag –
der Jahreskongress seit 1995

Prospects for EU-funded security research – The ethics of impact outside the EU discourse.

Caroline L. Davey
Andrew B. Wootton

From: Claudia Heinzelmann and Erich Marks (Eds.):
International Perspectives of Crime Prevention 9
Contributions from the 10th Annual International Forum 2016
within the German Congress on Crime Prevention
Forum Verlag Godesberg GmbH 2017

978-3-942865-73-9 (Printausgabe)
978-3-942865-74-6 (eBook)

Caroline L. Davey, Andrew B. Wootton

Prospects for EU-funded security research – The ethics of impact outside the EU discourse

1.0 SUMMARY

Established in 2004, the European Security Research Programme (ESRP) aims to grow Europe's security industry, as well as protect the EU from threats such as terrorism, disasters, organised crime and cybercrime. Created with support of the defence industry and large technology companies, the ESRP promotes technological solutions to security threats. The techno-military approach, considered successful in terms of improving EU industry competitiveness, has continued with the transition from the European Framework Programmes to Horizon2020. In this paper, the authors critically reflect upon the aims, approach and impact of the ESRP from a variety of perspectives. The EU is addressing thorny ethical and practical issues related to the ESRP – including data protection, privacy, meeting user needs, creating positive societal impact and inclusion. To widen participation in the ESRP, the EU funded the *SecurePAR*T project to support engagement of civil society in European security research. SecurePART identified concrete examples of civil society involvement in EU-funded security projects that helped address important security issues, focusing attention on practical solutions to problems that were tailored to the needs of practitioners. Although currently under-represented, civil society organisations (CSOs) have an interest in participating in the ESRP-funded projects – as long as such projects are compatible with their own interests and values. SecurePART made recommendations to increase CSO participation in the ESRP for the benefit of civil society. This paper contributes to the debate about 'value' and 'ethics' in the context of security at a European level, and is part of a wider body of literature on civil society and security.

2.0 INTRODUCTION

The 2016 GCOCP-Congress in Magdeburg on the theme "Prevention and freedom: On the necessity of an ethical discourse" highlighted the importance of discussing ethics in relation to security. At a European level, research projects on security are being delivered by the European Security Research Programme (ESRP), under the EU's Horizon2020 funding programme – formally Framework Programme 7. The ESRP addresses four main security themes: (i) crime and terrorism; (ii) natural and

manmade disasters; (iii) cybercrime; and (iv) border control. The ESRP is part of the EU's strategy supporting growth of the European security industry and promoting greater industrial competitiveness. In terms of ethics, the EU promises to "*improve security, whilst respecting fundamental human rights"* (EU Commission, 2016/2017). The ESRP adopts a business-focused, techno-military approach to security (Hayes, 2009), focusing on international threats – rather than everyday crime and security issues of concern to local communities. Technological solutions to problems are promoted, rather than social, design or system interventions.

An evaluation of the ESRP is not straightforward, since the programme can be looked at from a number of different perspectives. Framework Programme 7 has recently been evaluated by the Technopolis Group – a consultancy employed by the EU Commission to assess the programme and write an evaluation report (Technopolis, 2016a, b).

In contrast, this paper considers the ESRP from the perspective of civil society organisations (CSOs) – including those that may participate in EU-funded security research. CSOs, a term used by the EU Commission, are non-governmental, not-for-profit organisations that address societal issues. These include, for example, human rights, poverty reduction, and environmental issues. CSOs comprise a range of organisations – from grassroots movements, through law associations to emergency services (Europeaid, 2016). Insight into civil society perspectives on ESRP was obtained through participation in *SecurePART*, a 24-month project to support engagement of civil society in European security research (SecurePART, 2016). In order to better understand the ESRP, this paper also explores a CSO's account of its conception (Hayes, 2009).

The evaluation of the ESRP is structured into three main sections – each reflecting a different viewpoint. The first section outlines the ESRP and explains current funding calls within the context of the whole research programme. The authors illustrate the continuing dominance of the techno-military approach through reference to the 2016/17 Horizon2020 Security Programme funding call. The second section offers a critique of the ESRP from the perspective of the CSO *Statewatch* (Hayes, 2019). Drawing on research undertaken by Statewatch, the authors seek to understand how and why the techno-military focus came about. In the third section, the views of CSOs involved in EU security research are presented and the prospects for improving the ESRP considered – from widening participation, through revision of the programme to the inclusion of alternative calls (SecurePART, 2016).

This paper contributes to research and guidance on civil society, security and participation within Horizon2020 (Consider, 2013; Fondation Sciences Citoyennes, 2013). It is part of a wider body of literature on the role of civil society in governing business (Hutter and O'Mahony, 2004) and science (Bussu, 2015).

3.0 THE EUROPEAN SECURITY RESEARCH PROGRAMME

In 2004, the European Commission established a seven-year European Security Research Programme (ESRP) that aimed to deliver new security enhancing technologies to European Union's member states and to protect the EU citizens from threats. Known as the "Framework Programme", it addressed terrorism, organised crime, border control and disasters – and later also cybercrime. These types of security issues tend to cross national borders and therefore require some degree of international cooperation. The 'crime and terrorism' theme focused on organised crime, including the trafficking of human beings and narcotics. More everyday crime, which the programme refers to as "petty crime" has only been covered in more recent years.

The ESRP explicitly aimed to foster the growth of a profitable and globally competitive European 'homeland security' industry (Hayes, 2009). In 2016, the 7th Framework Programme was superseded not by the 8th Framework Programme, but by Horizon2020. Under Horizon2020, the ESRP has undergone changes compared to the Framework Programme, but remains oriented around improving industrial competitiveness.

The Horizon2020 security funding calls

The Horizon2020 security programme publishes a series of funding calls, to which project consortia are invited to respond (EU Commission, 2016/2017). The funding calls outline not only the security problem, but also the envisaged solution – usually a technology – and the expected impact. This is a 'top-down' approach where the funding body dictates the nature of the research by prescribing the approach, focus and expected impact. The funding proposals are reviewed by evaluators and administrators focussed on ensuring that funded projects clearly conform to the requirements outlined in the funding call. Most evaluators are experts in technology related fields, such as digital technologies and cybercrime.

The EU funding calls represent a technological viewpoint and generally involve development of technological solutions, as demonstrated by the call on border control. This call expects consortia to develop technology to detect people or vehicles along borders covered by forests, see box below.

BORDER CONTROL AND EXTERNAL SECURITY

SEC-16-BES–2017: Through-foliage detection, including in the outermost regions of the EU

Specific Challenge: Member States' authorities are carrying out activities all along the European border, and have started to share operational and situational information. But several regions at the borders of the European Union are covered with forests, and face extreme temperature conditions. Detecting, locating, tracking or identifying persons and vehicles crossing the border in forested regions is extremely difficult given that technologies for surveillance through harsh unstructured environments are currently not effective. The increasing risk of irregular flows and immigration across the border with, for instance, Turkey, Ukraine, Belarus, Russia or Brazil makes the issue even more acute than in the past.

Scope: Systems should be developed that combine or improve surveillance technologies and techniques and arrays of sensors of different sorts capable to provide higher quality detection capabilities and imaging via the integration of different techniques, to achieve wide- and small-area through foliage detection, despite the canopy density, in a real operational context. They could build on airborne, satellite-based, and/or on ground based platforms….Ethical and societal acceptance needs to be properly addressed. Whereas activities will have an exclusive focus on civil applications, coordination with the activities of the European Defence Agency (EDA) may be considered with possible synergies being established with projects funded by the EDA programmes. The outcome of the proposal is expected to lead to development up to Technology Readiness Level (TRL) 5 or 6.

Expected Impact:

Short term: Improved border surveillance and search-and-rescue capabilities, especially in forested regions;

Medium term: Validated through-foliage detection technologies, in terms of fitness for purpose, low rate of false alarms, practicability, mobility, and cost effectiveness.

Long term: Demonstrated through-foliage detection technologies in the context of realistic operational scenarios, in extreme weather conditions, to be implemented in collaboration with the relevant border surveillance authorities and in regions where the Frontex Agency indicates

The funding programme makes reference to human elements, but does not delve deeply into these factors. In the funding call on border control and external security, SEC-16-BES–2017, for instance, ethical issues are briefly mentioned. The primary

focus is on 'border control' ("no gate" border crossing, checking of goods during customs). Consequently, the funding call does not outline the need to tackle the causes of mass migration or address the humanitarian issues. Similarly, a technology approach is evident within the funding calls on crime and terrorism, disaster management and cybercrime. Furthermore, an analysis of the words used in the 2015/16 funding programme reveals the relatively high frequency of words such as 'technology', 'security' and 'defence' – compared to words that embrace human elements such as 'human factors' or 'citizens' (Davey and Wootton, 2016).

The economic impact of the ESRP

The ESRP is designed to deliver projects that promote Europe's economic prosperity – and its aims are explicitly stated. In the words of Bill Clinton's 1992 presidential campaign:

"It's the economy stupid"

But will the ESRP help to improve the European economy? And, if so, is this the type of publically-funded research programme that we want in Europe? Security research funded under the EU's 7th Framework Programme has been evaluated by a research consortium led by Technopolis Group – a consultancy specialising in the evaluation of policy initiatives (http://www.technopolis-group.com/about/). Commissioned by the European Commission, the evaluation assesses the 7th Framework Programme against its aims and objectives. The results have been published in a 235-page report – *"Final Evaluation of Security Research Under the Seventh Framework Programme for Research, Technological Development and Demonstration"*. An executive summary is also available (Technopolis Group, 2016a, b).

According to Technopolis Group, research projects are impacting on policy and industry:

"Around 20% of respondents have seen or expect to see their project result in policy outputs, market applications and standards, and new patents" (Technopolis Group, 2016, p. 4, Executive summary).

Technopolis Group state in the executive summary that the Framework Programme 7 has had a positive impact, especially in relation to developing technology – and that this is a widely-held conclusion:

"It is concluded that the Security Research Programme has had a positive impact on each of its specific objectives. The great majority of participants (75%+) hold this opinion… a greater share of participants believes the programme has made a substantial contribution to the 'developing technology to build capability' objective (85%)" (Technopolis Group, 2016b, p. 4).

The authors of the evaluation go on to conclude that the Programme can be considered a success in terms of achieving its primary objective – to improve the European security industry:

"The evaluation team concludes that the programme has had a significant impact on the EU's security industry and is improving the global competitiveness of the EU's security industry. A majority of participants believe that the impact has been at least medium if not high." (Technopolis Group, 2016b, p. 4).

However, the 7th Framework Programme was primarily evaluated in terms of its delivery and economic impact. Furthermore, the findings come from surveys and interviews with project and programme participants – who are in effect being asked to assess their own research projects.

In the full report, some reservations about the 7th Framework Programme's contribution to industrial competitiveness are highlighted. It is noted that:

"there were reservations expressed about the absolute suitability of the Framework Programme model as a means by which to support industrial innovation" (Technopolis, 2016a, p. 24).

The reservations are attributed in part to the long timescales for project funding, making the programme less suited to product development activity. For example:

"One senior industrialist remarked that… it perhaps makes more sense to focus on more fundamental issues where progress may well benefit from the longer gestation period and ability of these innovation platforms to convene larger groups." (Technopolis Group, 2016a, p. 24).

Amongst academics, it was admitted in the full report that concerns were expressed more frequently about the focus on industry interests and on applied research for projects looking to bring technologies to market. This appears to impact negatively on the quality of the research knowledge being generated by EU-funded security research projects:

"There was a single widely expressed reservation: the decision to focus on very applied, near-term projects made the calls a little more relevant to industry and end-users and a little less relevant to the interests of the public research base. The academic community would have preferred more opportunities for carrying out rather more fundamental research." (Technopolis, 2016a, p. 24).

Academics were concerned that the type of research and the focus on developing practical solutions limited the scope for peer-reviewed academic journal papers – the main method for sharing knowledge within academic circles.

The Technopolis Group does not critically evaluate the 7th Framework Programme, nor does it reflect upon the aims and objectives of the ESRP. Such a critique would clearly be outside of its brief. However, a critical evaluation has been undertaken by Statewatch.

4.0 THE STATEWATCH CRITIQUE

Founded in 1991, Statewatch is a not-for-profit organisation that monitors the state, justice and home affairs, security and civil liberties in the European Union. Working for Statewatch are a range of professionals including: lawyers, academics, journalists, researchers and community activists. Together with the Oslo Peace Institute, Statewatch has researched the ESRP – raising questions about its conception, delivery and impact (Hayes, 2009). Statewatch are particularly concerned about increased surveillance by the state (Hayes, 2006).

Impulse for the ESRP

According to Hayes (2009), the ESRP was inspired by spending in the USA on security research. The proposal was to allocate 1.4 billion EUR (for 450 million Europeans) – which would represent a rate of security research funding similar to the USA. However, less was allocated to the budget. It should have been a minimum of 1 billion EUR per year, but ended up being 200 million per year for FP7 (although there is extra for space research).

The 'Group of Personalities'

The ESRP was set up by a group of senior managers from industry, the military, research and the EU. In 2003, the 'group of personalities' (GoPs) – as it was known – came together to develop the EU Security research programme. This Group of Personalities comprised (Hayes, 2009):

- EU Commissioners (and four members of the European Parliament)
  – European Commissioners for Research and Information Society;
  – the Commissioners for External Relations and Trade;
  – the High Representative for the EU's Foreign and Security Policy;
- The military
  – NATO; the Western European Armaments Association; and the EU Military Committee;
- Eight multinational companies:
  – Europe's four largest arms companies (EADS, BAE Systems, Thales and Finmeccanica);
  – Europe's largest IT companies (Ericsson, Indra, Siemens and Diehl);
- Seven research institutions, including the Rand Corporation.

As Hayes (2009) points out, civil society organisations (CSOs) were under-represented within the Group of Personalities. A number of 'Think Tanks' were involved – i.e. Research or policy institutes that undertake research and advocacy concerning topics ranging from social policy, through economics to technology. According to Hayes, these institutions were not critical of the approach or vision adopted within the ESRP.

The ESRP appears to have been defined in just two meetings (Hayes, 2009) and presented within a *"Preparatory Action for Security Research"*. Interestingly, there was no public consultation and no 'green paper'. In the European Union (and in some countries, such as the UK and US) a 'green paper' is generally produced. This is a "tentative government report" and consultation document of policy proposals for debate and discussion (EUR–Lex, Green Paper, accessed 14.10.16).

Legal basis for the research programme

The legal basis of the research programme was Article 157 of the EC Treaty on the 'competitiveness of the Community's industry' – as opposed to Article 163 on 'research and technological development'. Article 157 states that:

"The Community and the Member States shall ensure that the conditions necessary for the competitiveness of the Community's industry exist." (EUR–Lex, Article 157, accessed 14.10.16).

According to Article 157, the action of the EU Commission and member states should be aimed at speeding up the adjustment of industry to structural changes, promoting initiative (particular in relation to small and medium-sized enterprises), encouraging cooperation between enterprises and supporting industry exploitation of innovation policies, research and technological development.

In contrast, Article 163 of the EC Treaty states that:

"The Community shall have the objective of strengthening the scientific and technological bases of Community industry and encouraging it to become more competitive at international level, while promoting all the research activities deemed necessary by virtue of other chapters of this Treaty." (EUR–Lex, Article 163, accessed 14.10.16).

According to Article 163, the European Community should support the development of high quality activities amongst research centres and universities. It should also help them *"exploit the internal market potential"*, in particular through the opening-up of national public contracts, the development of common standards and the removal of legal and fiscal barriers to cooperation (EUR–Lex, Article 163, accessed 14.10.16).

In addition, the research programme was developed under the auspices of the Commission's Directorate-General for Enterprise – and not Directorate-General for Research. The latter was the established Research & Development (R&D) arm of

the Commission, responsible for EU research and innovation policy and coordination activities (Hayes, 2009).

According to Hayes (2009), the choice of legal basis for the research programme reflected the focus on promoting industrial competitiveness:

"The goals of the DG Enterprise (industrial competitiveness and long-term profits) were more important than those of its R&D counterpart (the creation of a 'knowledge society'). (Hayes, 2009, p. 9).

The EU security-industrial complex

Hayes (2009) notes that the ESRP was explicitly designed to support transfer between military and civil contexts, in that it aimed to:

"Bridge the gap between civil and traditional defence research, foster the transformation of technologies across the civil, security and defence fields and improve the EU's industrial competitiveness." (Hayes, 2009, p. 10).

'Civil' relates to the concerns and governance of ordinary citizens – as opposed to the military. The Group of Personalities (2004) highlighted 'synergies' between the (military) defence and (civil) security sectors. The group argued that technology is potentially multi-purpose and has applications across defence, security and civil society.

"Technology is very often multi-purpose. Civil and defence applications increasingly draw from the same technological base and there is a growing cross-fertilisation between the two areas... As a result, the technology base for defence, security and civil applications increasingly forms a continuum... applications in one area can often be transformed." (Hayes, 2009, p. 11).

The Group of Personalities considered technology vital for security:

"Technology itself cannot guarantee security, but security without the support of technology is impossible. It provides us with information about threats, helps us to build effective protection against them and, if necessary, enables us to neutralize them." (Hayes, 2009, p.11).

Furthermore, the group argued that a techno-military approach to security would benefit policymakers and ordinary citizens alike. Security, terrorism, proliferation of weapons of mass destruction, failed states, regional conflicts, organised crime and illegal immigration were considered sources of anxiety for both citizens and policymakers.

The EU's bringing together of security and industry within the ESRP is defined by Hayes (2009) as the *"security-industrial complex"* (p. 11). Hayes (2009) points out

that there is a strong economic case for subsidising the development of the security-industrial complex in Europe. It is better for European governments to procure security technology and equipment produced within Europe – rather than America – and to potentially enable European corporations to benefit from the global market for security technologies.

The defence industry in the ESRP – level of influence

To evaluate the influence of the defence industry on the ESRP, Hayes (2009) looks at their participation, comparing Phase 1 with Phase 2 of the ESRP: Phase 1, 2004 to 2006; and Phase 2, 2007 to 2013. In 2014, Horizon2020 was launched.

In Phase 1 of the ESRP (2004 to 2006), the defence industry had a key role to play in the development and delivery of research projects. Of the 39 security research projects, 23 (60%) were led by companies that primarily service the defence sector. Furthermore, the defence sector participated in 26 (67% or two-thirds) of the 39 projects.

In Phase 2, 2007 to 2013, of the 46 Framework Programme 7 security research projects funded under the 2007 call, 17 (or 37%) were led by organisations that primarily service the defence sector, with a further five led by corporations from the security industry.

On the surface, it would appear that the defence sector was less dominant than in Phase 1. However, the defence sector was involved in the majority of projects, notes Hayes (2009). Furthermore, there were no civil society organisations (CSOs) leading EU security projects in Phase 2.

Obscuring of the industry-technology nexus

Hayes (2009) observes changes in style of presentation within the funding documents produced for Phase 1 compared to Phase 2. In Phase 2, the ESRP was presented in a few pages and therefore contained "none of the substance" (p. 18). As a result, the technology focus and economic/commercial drivers are less apparent to the reader and the potential for debate reduced:

"The security research component of FP7 provides a master class in how to prevent debate by substituting specific proposals for generalities, and disguising the aims with the means… To read the FP7 programme on its own, with its stated commitment to civil liberties, privacy, fundamental rights and democracy, unseasoned observers will find little cause for concern." (Hayes, 2009, p. 18).

Hayes (2009) goes on to highlight the inclusion of key ideas and 'liberal values', without clarity on how their contradiction with industry-technology focus will be addressed.

Looking in-depth at any of these liberal values and ideals is quarantined to individual projects. In this respect, a number of projects are highlighted including: The PACT, PRISMS and SurPRISE projects under grant agreements no. 285635, 285399 and 285492 respectively. (For further information see: OEAW website, accessed 28.11.1). This obscuring makes it harder for researchers involved in EU security research to understand or critique the programme.

Within the ESRP, it is assumed that security can be achieved without undermining fundamental human rights. The challenge associated with attempting to achieve different objectives or address conflicting interests is ignored or downplayed. The expectation on EU researchers to believe in both security and fundamental human rights – and to ignore any contradictions between the different sets of beliefs could arguably be likened to George Orwell's concept of "Doublethink". This is defined as:

"The power of holding two contradictory beliefs in one's mind simultaneously, and accepting both of them." (George Orwell, "Nineteen Eighty-Four")

Indeed, modern examples of doublethink often appear within the field of security, including: "*Peace-keeping force*" *and* "*fighting for peace*".

In psychological terms, doublethink is associated with 'cognitive dissonance' – that is the mental stress or discomfort experienced by an individual who holds two or more contradictory beliefs, ideas, or values at the same time.

5.0 CONCRETE STEPS TO IMPROVE THE ESRP

In an attempt to improve the ESRP, and respond to its critics, the EU has engaged a number of relevant, but underrepresented, groups in the programme and paid greater attention to human factors associated with technology solutions.

Reaching out to SMEs

The ESRP was set up with support from large technology companies and the defence sector; a situation that is considered to disadvantage small and medium-sized enterprises (SMEs). In response, various methods have been adopted to increase SME involvement and promote economic growth: consortia have been encouraged to include SMEs as partners; financial and administrative procedures have been adapted to the needs of SMEs; and specific funding calls have been developed to support SME-led projects.

Reaching out to practitioners

The ability of the ESRP to develop practical solutions to real security threats is a priority for the EU. In recent years, attention has therefore turned to encouraging greater participation amongst 'practitioners' – i.e. professionals who are users of

security technologies. The aim being to improve the relevance and usability of solutions arising from EU-funded security projects.

Considering the human element

There has been some attempt to better understand the needs and requirements of users and/or practitioners. The ESRP is very much technology-led – that is, it is focused on supporting technologies that can be leveraged to solve a customer need. It would appear appropriate to assume that the technology innovation already exists and that industry or the military is simply seeking a market. Such an approach may be considered appropriate for large-scale innovations in the field of security, but it does tend to assume that technology is 'the solution'. A technology-led approach contrasts with customer-led innovation, where the product or service is developed after gathering customer insight (Inventium, 2015).

To counter criticisms levelled at technology-led approaches the EU has included funding calls focusing specifically on the 'human factor' and asked that projects take into account issues such as privacy and societal impact.

Including non-standard funding calls

Interestingly, some funding calls within the ESRP do appear to lie outside the norm. In 2016/17, for instance, there were funding calls to tackle domestic violence and high impact 'petty' crimes, as well as funding calls focusing on developing non-technological solutions such as tools or guidelines. The funding call on engaging civil society in security research also lies outside of the norm.

6.0 CIVIL SOCIETY ORGANISATIONS IN EU SECURITY RESEARCH

The final Framework 7 Programme contained a funding call focussing on engaging with 'civil society organisations' – CSOs. CSOs are non-governmental, not-for-profit organisations that address societal issues such as human rights. As an extract from the funding call demonstrates, the EU wanted to commission a project to develop a strategy for enabling CSOs to both participate in security research projects and shape the ESRP, see box below:

Topic SEC-2013.7.3-1 Increasing the engagement of civil society in security research – Coordination and Support Action (Supporting Action)

Description of topic:

"…A strategy should also be developed with concrete action steps how to increase their participation in both the shaping and the implementation of civil security research. Also, steps should be considered on how to ensure a greater understanding among civil society organisations of the potential benefits, especially with regard to societal security, of the results coming from security research activities."

[SOURCE: Original FP7 call]

This led to a 24-month project to identify strategies to engage civil society organisations in European Security research – called *SecurePART.* The project consortium comprised Bantec Group (ES), ENNA (BE), vdl Consult (DE), Nexus (DE), Goethe Universität (DE), University of Salford (UK) and Loba (PT). SecurePART was led by Bantec – a spanish-based consultancy. Nevertheless, a CSO, the *"European Network of National Civil Society Associations"* (ENNA) had a leading role in engaging with CSOs, supporting research and developing the project's communication strategy. Based in Brussels, ENNA brings together organisations, platforms and associations working at a national level to promote the cross-sectoral interests of the civil society sector. This sector addresses a range of social and environmental issues, and also promotes socio-cultural activities. Since ENNA engages with national CSO representatives, rather than CSOs themselves, it describes itself as an *"umbrella of umbrellas"*. ENNA works directly and indirectly with over 80,000 local, regional and national civil society organisations (ENNA, 2016).

In the funding proposal, the consortium proposed to support civil society involvement in European security research, as well as promote consideration of non-technological solutions to security problems – and promote social innovation.

"The main goal of the SecurePART project is to contribute to stronger engagement with and involvement of civil society organisations and their advocates in EU security research in order to advance the dimension of non-technological, social innovation." (SecurePART funding proposal).

This was justified on the grounds that it would lead to better, more comprehensive security solutions:

"Technological research and innovation, despite its advantages for the European

market and economy, is not a sufficient solution to comprehensive security problems faced by contemporary European societies." (SecurePART funding proposal).

Defining and researching CSOs

The European Commission uses the term "civil society" and "*Civil Society Organisation"* – or CSO. The term Non-governmental Organisation (NGO) is also commonly used. To be able to deliver the project, the SecurePART team first had to agree on a definition for a CSO. According to EU Commission sources (Europeaid, 2016), CSOs are organisations that are non-governmental, voluntary and support citizens in their efforts to act and promote common interests. CSOs include:

- Grassroots initiatives seeking to bring about social changes
- Organisations active in fields such as poverty reduction, emergency response, human rights, environment, etc.
- Cooperatives, trade unions, professional associations (if not compulsory).

CSO representation with ESRP

Detailed information on the involvement of CSOs within the ESRP was not available. During the first phase of the SecurePART project, research was therefore conducted to identify the representation of CSOs within the ESRP from 2007 to 2013 (Balzer and Henseler, 2015). To do this, the consortium partners analysed the EU's CORDIS database – i.e. The "Community Research and Development Information Service". All EU-funded projects should be listed on this online database (http://cordis.europa.eu/projects/home_en.html).

From CORDIS, SecurePART researchers identified 1,935 projects, coordinators and partners in the field of security. CSOs are not identified explicitly on CORDIS, but are simply listed as 'other' – i.e. not private companies or research institutions. Project partners therefore had to examine all organisations listed as 'other' to identify whether they might be defined as a CSO. This involved reading and sometimes translating the project and organisation websites.

SecurePART found that of the 1,935 projects, only 39 contained participants that fell completely within the CSO definition. However, there were a further 26 that were almost within the definition – 'hybrid' CSOs. There were also 20 that were technically outside the CSO definition, but shared many of the characteristics of CSOs. As shown in SecurePart Policy Brief 1, CSOs continue to be under-represented within the ESRP from 2007 – 2013 (Balzer and Henseler, 2015). In fact, only 4.8% of participants were CSOs.

CSOs involved in the ESRP

SecurePART researchers identified CSOs involved in the ESRP – from first responders in crisis situations through human rights and citizen participation associations to

organisations concerned about passenger safety. Those who respond to emergencies are the group of CSOs most involved in the ESRP: the Red Cross and similar organisations; emergency services – including fire brigade, first aid and rescue services; medical associations, such as Medicins Sans Frontieres. These CSOs were often involved in projects on crisis and disaster management.

Some CSOs worked on behalf of civil society, representing citizens' interests, human rights, consideration of legal and ethical issues or environmental protection, often focusing on particular fields – including science, transport and ICT. Such CSOs might advise a research project consortium on the impact of security technologies on users, citizens, wider society or the environment. Other CSOs actively promote the involvement of civil society in security research by providing a forum for citizens and public sector organisations.

In addition, there were independent research organisations – or 'think tanks' – that contribute to public policy through research into social and environmental issues. (For further information on the groups of CSOs, see Kolliarakis *et al* (2015) SecurePART Deliverable 3.2).

The contribution of CSOs to the ESRP

Through a series of case studies, SecurePART was able to identify three main modes for CSO involvement in EU-funded security research projects and their associated benefits. These benefits related to individual CSOs, a specific research project and/or the overall Programme.

1. CSOs leading projects to address key security issues

There are a number of CSOs that are playing an important role in relation to the ESRP in that they are able to lead research projects. Such CSOs are able to bring together consortium partners, write and shape funding proposals and act as project co-ordinator on EU-funded projects. There are also CSOs that do not lead research projects, but nevertheless take on a partner role, and contribute significantly to the project's aims, approach and outputs.

In addition, a small number of CSOs are helping to shape the ESRP through involvement in key projects, acting in an advisory capacity to the EU Commission or participating in the EU's Security Advisory Group. Advisory groups enable expert input in relation to the Horizon2020 research programme. Since 2016, the security advisory group is titled the *'Protection and Security Advisory Group'*.

An example of a CSO leading EU projects on security is the 'Institute for Strategic Dialogue' (ISD). This is a UK-based think tank specialising in preventing and responding to violent extremism. While ISD addresses major social and security challenges, it has developed particular expertise in preventing and responding to

violent extremism (http://www.strategicdialogue.org/about-us/). ISD is involved in reaching out to communities and to persons attracted to violent extremist groups. This is a difficult process. The status of a CSO, especially those that are community-led, confers a number of benefits. A CSO is more readily accepted and trusted by former extremists and other organisations working in the field. Indeed, CSOs tend to be perceived as 'independent' and considered to have a legitimate role to play in tackling social issues (Davey and Wootton, 2016a).

ISD participation in EU-funded research projects has led to the development of practical resources of value to policy makers and practitioners, including short films to communicate with key groups and learning materials that are accessible to practitioners. ISD has also developed and launched a searchable, up-to-date repository for information about government policies and programmes. This online resource is helping policy makers, practitioners and academics exchange information, share examples of good practice and stay in touch and remain up-to-date with latest developments (http://www.strategicdialogue.org/programmes/counter-extremism/counterextremism). ISD is also playing a key role in coordinating activities between stakeholders, through its participation in networks, such as Against Violent Extremism (AVE) (AVE website, 2016; Davey and Wootton, 2016a).

In some instances, research and interventions delivered by ISD involves technology companies. Against Violent Extremism was developed in collaboration with Google Ideas in 2011 (AVE website, 2016). In partnership with Facebook, ISD is tackling the challenge of hate speech and violent extremism on social media. (Further information about the Online Civil Courage Initiative (OCCI) launched in Germany in 2016 is available at: https://www.facebook.com/onlinecivilcourage). ISD is also tracking and archiving social media material related to female profiles involved in so-called Islamic State across online platforms such as Twitter, Facebook and Tumblr. The aim being to give a *"unique lens into the daily lives of foreign women living in the so-called Islamic State"*. Thus, a focus on technology appears to be adopted in situations where the approach is of real value in understanding and countering violent extremism.

2. CSOs delivering research, events and solutions of practical value

There is a small, but important group of CSOs for whom EU-funded security research is delivering outputs and networking opportunities of value to the CSO and its members. Opportunities to network and share good practice on disaster management are welcomed by Red Cross organisations, such the Austrian Red Cross (van der Lippe, 2016) and the Israeli Magen David Adom (Almeida, 2016).

Security is also important to a range of organisations concerned with the urban environment and public services. The European Forum for Urban Security (Efus) is helping its local authority members learn about technology solutions to security issues, including CCTV (Davey and Wootton, 2016b). Efus was a partner on an EU project

on surveillance, ethics, legal issues and efficiency – called SURVEILLE. This project enabled local authority Efus members to reflect on the use of technologies for urban security – from CCTV to other technologies introduced in so called 'Smart Cities'. Smart city approaches seek to manage the urban development by integrating multiple information and communication technology (ICT) and Internet of Things solutions. Efus members are amenable to the use of technology in improving security where the benefits outweigh the costs, the technology complements other approaches and it does not prevent more complex causes being addressed (Efus Manifesto, 2012, p. 27). Through SURVEILLE, local authorities were able to examine the effectiveness of CCTV and other solutions, as well as discuss ethical and human rights issues relating to the practical use of technology in the context of their town or city. According to Efus, the project created a mutually beneficial exchange between researchers of different disciplines, local decision-makers and practitioners. Furthermore, the insights from the project have led Efus' Executive Committee to adopt a resolution on technologies and urban security at the Efus general assembly in Paris in 2012 (Efus, 2012).

3. CSOs inputting on ethical and human rights issues

Through their participation in EU-funded security projects, CSOs with specialist expertise are providing input on a range of issues including: ethics; privacy; human rights; emerging technologies; and relevant global-political perspectives. In so doing, they are attempting to reduce the potential negative impact relating to technological solutions to security issues. For instance, the Law and Internet Foundation in Bulgaria is helping research consortia identify ways in which security technologies may undermine human rights or raise ethical issues. Where possible, the Law and Internet Foundation recommends alternative methods and technologies that preserve privacy (Kolliarakis and Ochs, 2016). Other types of CSO promote greater consideration for societal issues by supporting project consultation with CSOs and/or citizens. Such engagement potentially widens the perspective of project consortia concerned about public acceptance of new technologies.

7.0 SECUREPART STRATEGIES FOR IMPROVING THE ESRP

Improvements might come from greater involvement of CSOs within the ESRP. However, it was noted the more significant developments would require some revision to the funding calls. The SecurePART project therefore advocated various strategies to help transform EU-funded security research.

The benefits of engaging CSOs in security research

SecurePART findings suggest that the involvement of CSO in security research can impact positively on research project outputs. The value of CSO involvement in EU-funded security research included: support for development of practical solutions to

security issues; use of technology where appropriate; more attention on user and practitioner needs; greater consideration of ethical and human rights issues; support for engagement with users, citizens and key stakeholders groups.

SecurePART took measures to increase the representation of CSOs in EU-funded security research. In particular, SecurePART produced guidance for CSOs, brought together CSOs and other key stakeholders involved in the ESRP in events and presented recommendations to the EU Commission for engaging with CSOs. These documents are available from the project website (www.securepart.eu). Importantly, with the support of the CSO partner ENNA, SecurePART was able to identify and engage with CSOs who wanted to be involved in EU-funded security research. The CSOs were identified through a survey of ENNA members, interviews, workshops and seminars.

Offering alternative funding calls

Amongst interested CSOs, there were those for whom the ESRP seems to offer relevant and feasible options for participation. However, there remain barriers to further involvement amongst CSOs. A SecurePART workshop in Berlin, Germany (2015) found that CSOs are concerned about the ESRP's focus on industry interests and its supports for technology solutions to security. Indeed, some CSOs find the ESRP approach 'alienating' – in that it makes them feel unconnected to the ESRP, even perhaps actively excluded.

Furthermore, the techno-military approach adopted by the ESRP raises ethical and human rights issues for CSOs. CSOs fear that they might be used to conceal controversial aspects related to EU security research. In other words, CSOs are worried about being used as a 'fig leaf', so that problems and issues can be glossed over:

> "a leaf of a fig tree, often used for concealing the genitals in paintings and sculpture", or "a thing intended to conceal a difficulty or embarrassment" (dictionary definition).

This point was raised in the *SecurePART Action Plan for Strengthening links between Civil Society Organisations and Security Research* (SecurePART, 2016).

"It is worth remarking that 'participationism' has become for many public sector organisations a kind of panacea in order to amend legitimacy gaps, or overcome acceptance problems. However, CSOs regularly suffer from participation fatigue, realising that their engagement often results in no substantial influence, and that their presence gets instrumentalised as a tickbox exercise for public administration, turning them into a 'fig leaf' for policies serving other interests than the public good." (SecurePART, 2016, p. 4).

To enable real engagement with CSOs, and improve the ESRP, the SecurePART consortium proposed alternative funding calls designed to address security issues from the perspective of civil society. In addition, open calls were proposed as a method for encouraging a wider range of research projects and supporting innovation. These were presented to the EU Commission.

8.0 DISCUSSION AND THE WAY FORWARD

While concrete steps have been made to improve the ESRP, it should be noted that improvement is an ongoing process. In this respect, the 2016 GCOCP conference was a welcome opportunity to reflect upon the way forward for the ESRP.

A broader range of issues

Significant public funds are being invested in research and development of technological solutions that aim to counter terrorism, manage borders, respond to disasters and tackle cybercrime. During the initial phase of the ESRP, this left limited scope for research into tackling the daily crime and insecurity problems facing citizens or developing socially-oriented innovations. These daily crime and insecurity issues are a major concern for citizens – even those living in countries with a comparatively high risk of terrorism. In the 2016/17 funding call, the ESRP covered a range of issues that impact on citizens safety, security, wellbeing and quality of life, including domestic violence and everyday crimes – referred to as 'petty' crime in the funding call. Further coverage of these important issues should be considered.

Developing practical solutions

Technology has proved effective in preventing a range of everyday crimes impacting on citizens and wider society. For instance, technological advances in security have reduced theft of vehicles across Europe, without impacting negatively on the user (van Dijk et al, 2012; Farrell, 2013). However, crime prevention is achieved through a wide range of interventions. The authors suggest that better security requires openness to solutions with potential real world impact – regardless of whether technology, design, social, legal or policy-oriented.

A more critical approach to technology solutions

The ESRP has focused on the development of technology solutions – rather than on supporting more fundamental research. However, there is a danger that technology solutions might impact negatively on citizens and wider society. The ESRP might consider supporting research into user needs and the societal aspect of security. This research should be focused around topics relevant to the ESRP.

Design innovation

The ESRP should be supporting innovation in the field of security. By 'innovation', the authors are referring to the development of ideas with potential to solve real-world problems – as opposed to simply 'novel' ideas. However, the ESRP funding calls are generally fairly prescriptive, with solutions already prescribed in the call text – meaning a consortia cannot suggest alternative or better ideas. This prescriptive, planned way of thinking may be typical of the military sector, defence industry and some engineering professions, but less so in other disciplines or sectors – such as design.

The authors suggest that innovation might be supported through greater involvement of the design profession in the ESRP. Designers are creative when it comes to tackling problems, developing the best ideas, and prototyping them. In addition, designers are focused on the user, understanding the context and on the achievement of multiple (often competing) objectives, such as freedom and security.

Creativity is not the preserve of designers, of course. CSOs can be creative in their commitment to address security issues. An example is the Exit Deutschland programme for countering the Far Right in Germany. Exist Deutschland has developed innovative methods to persuade party members to leave the organisation. For instance, Exit gave away heavy metal style T-shirts to party members that, when washed, reveal a statement from Exit offering to support the wearer in leaving the party.

"Exit Deutschland handed out T-shirts that featured skulls and bones and the message "Hardcore Rebels: National and Free" on the front. However, after the first wash, the original design would wash away, revealing the hidden message underneath: "What happened to your shirt can happen to you. We can help you break from right-wing extremism." (O'Brien, 2016)

The T-shirts were referred to as "Trojan T-shirts" (O'brien, 2016). Academics and lawyers also have much to contribute when it comes to framing problems and fighting for justice.

Technology-enabled innovation

There are truly innovative uses of technology, where advantage is taken of specific technological capabilities in the design of solutions that meet users' needs. In the US, rape and sexual assault on university campuses is a significant issue – but victims may be reluctant to report incidents and accusations may be poorly handled by university staff. An ICT system has been developed for victims to record the details of a rape or sexual assault soon after occurrence. This information can then be used, if the victim later decides to report the incident to authorities. If the named offender is identified by a second victim, the case is automatically reported to the police for investigation. Discovering that another person has also been victimised is a 'game changer' for most individuals, justifying the person being reported to the authorities (Ladd, 2015).

Rethinking technology

In referring to technology, the ESRP is primarily considering digital technologies, computers and electronics – even though technology is more broadly defined as:

> 'Technology ("science of craft", from Greek τέχνη, techne, "art, skill, cunning of hand"; and -λογία, -logia) is the collection of techniques, skills, methods and processes used in the production of goods or services or in the accomplishment of objectives, such as scientific investigation." *(Dictionary definition).*

This narrow focus on digital technology relates to the value placed on technology in a generation where economic development is associated with knowledge, creativity and intellectual property. Suarez-Villa, in his 2012 book "*Globalization and Technocapitalism: The Political Economy of Corporate Power and Technological Domination*", relates a technology-focused, capitalist economic system – technocapitalism – to globalisation and to the growing power of technocapitalist corporations. He suggests that a "techno-military-corporate complex" is rapidly replacing the old "military-industrial complex" of the second half of the 20th Century. The liberal left in Europe has largely affiliated itself with such "technocapitalist" and neoliberalist approaches since the 1990s (Chakrabortty, 2016).

A human-centred, European approach

The unexpected outcomes of the 2016 UK Brexit vote and US presidential election, appear to signal that now may be a good time to revisit the neoliberal thinking some claim underpins Horizon2020 (Hayes, 2009). Other key developments that might drive a rethink are international problems (refugees, global terrorism, etc.) and concerns expressed by European citizens (anti-immigration sentiment, response to bulk surveillance revelations, etc.). Indeed, the planned and potential exit of member states from the EU may initiate a more engaged debate and increase the appetite for reform.

The ESRP seeks to tackle complex issues involving often interwoven sociotechnical systems (STS). The authors suggest the ESRP needs to better support the generation of insight and innovation around 'problem framing' (i.e. the construction and presentation of complex issues) and emphasise addressing the breadth of citizens' needs and requirements (i.e. adopt a human-centred perspective). These strategies should be prioritised over the use of specific tools and technologies that may or may not be appropriate. In this respect, the authors suggest the priorities of the ESRP must evolve, with the programme putting people and humanistic "European values" at its heart and focusing on social cohesion and human-centred solution development.

9.0 REFERENCES

Almeida, A. (2016) "CSOs in Security Research. Magen David Adom". SecurePART Policy Paper number 7, CSOs in Security Research. SecurePART project website. Available from: http://www.securepart.eu/download/securepart_pb-7160203174553.pdf

AVE website (2016, accessed 15.11.16) "About Against Violent Extremism", Against Violent Extremism website, managed by the Institute of Strategic Dialogue, available from: http://www.againstviolentextremism.org/about

Balzer, F. and Henseler, C. (2015) "State of the art Civil Society Organisation (CSO) participation in the European security research programme". Policy Brief No. 1. SecurePART project website. Available from: http://www.securepart.eu/download/securepart_pb-1160119150839.pdf

Bhusan Das Gupta, J. (2007) Science, Technology, Imperialism, and War. Pearson Education: India

Bussu, S. (2015) "Public Dialogue in Science and Technology: An International Overview". Sciencewise. Expert Resource Centre. March 2015

Chakrabortty, A. (2016) You're witnessing the death of neoliberalism – from within. The Guardian. Economics: Opinion section, Tuesday 31 May 2016. Available from: http://www.theguardian.com/commentisfree/2016/may/31/witnessing-death-neoliberalism-imf-economists

Consider (2013) European Policy Brief. Civil Society Organisations in Designing Research Governance (CONSIDER). EU project funded under Framework 7 programme (2012 - 2015 led by Carsten, B. De Montfort University. Available from: www.consider-project.eu

CORDIS (accessed 15.11.16) "Community Research and Development Information service" (CORDIS) database. Available from: http://cordis.europa.eu/projects/home_en.html.

Davey, C.L. and Wootton, A.B. (2016a) CSOs in Security Research. Institute for Strategic Dialogue (UK). SecurePART Policy Paper number 9, SecurePART project website. Available from: http://www.securepart.eu/download/securepart_pb-9160307121106.pdf

Davey, C.L. and Wootton, A.B. (2016b) CSOs in Security Research. European Forum for Urban Security. SecurePART Policy Paper number 8, SecurePART project website. Available from: http://www.securepart.eu/download/securepart_pb-8160503092825.pdf

Davey, C. L and Wootton, A.B (2016c) Prospects for EU-funded security research – The ethics of impact outside the EU discourse. Presentation at 2016 conference 'German Congress on Crime Prevention' (GCOCP), Magdeburg, Germany. Available at: http://www.praeventionstag.de/nano.cms/vortraege/id/3340

Efus (2012) *"Security, Democracy and Cities Manifesto: The Aubervilliers and Saint-Denis Manifesto".* European Forum for Urban Security: Paris, France. Published in various EU languages, and available for download from: http://efus.eu/en/resources/publications/efus/3779/

Efus website (accessed 09.11. 2015) "Efus partner of the research project on ethics and efficiency of surveillance technology "SURVEILLE". Available from: http://efus.eu/en/topics/tools-and-methods/technologies/news-surveille-project/efus/2665/

ENNA (2016, accessed 26.10.16) "*ENNA. Our Mission*". European Network of National Civil Society Associations (ENNA) website. Brussels, Belgium. Available from: http://www.ennaeurope.org/about-enna/our-mission/

EU Commission (2016/17) Horizon2020 2016 to 2017 Work Programme. Protecting freedom and security of Europe and its citizens. Available from EU Commission website: http://ec.europa.eu/research/participants/data/ref/h2020/wp/2016_2017/main/h2020-wp1617-security_en.pdf

EUR–Lex (14.1016) "Green Paper". Available from: http://eur-lex.europa.eu/summary/glossary/green_paper.html

Europeaid (accessed 28.11.16) Civil Society. International Cooperation and Development. Building Partnerships for Change in Developing Countries, Europe Aid, EU Commission: http://ec.europa.eu/europeaid/civil-society_en

Farrell, G. (2013) "Five Tests for a Theory of the Crime Drop". Paper presented at International Symposium on Environmental Criminology and Crime Analysis (ECCA), Philadelphia, US

Fondation Sciences Citoyennes (undated). Why and how to participate in the European Research and Innovation Framework Programme Horizon2020. Manual for Civil Society Organisations. Edited by Neubauer, C. Fondation Sciences Citoyennes; Paris, France

Garcia, B. M. (2014) *A Preliminary Report on Research Performing Organisations in the European Union*. Consejo Superior de Investigaciones Cientificas, CSIC Brussels Office. 12 June 2014.

Group of Personalities (2004) "Research for a Secure Europe". Report of the Group of Personalities in the field of Security Research. European Communities: Brussels, Belgium. Available from: http://ec.europa.eu/dgs/home-affairs/e-library/documents/policies/security/pdf/gop_en.pdf

Hayes, B. (2006) “Arming Big Brother: The EU’s Security Research Programme”. Amsterdam: TNI/Statewatch. Available from: http://www.statewatch.org/analyses/bigbrother.pdf

Hayes, B. (2009) “NeoConOpticon The EU Security-Industrial Complex”. Statewatch (UK) and Transnational Institute, TNI (Netherlands). Available from: http://www.statewatch.org/analyses/neoconopticon-report.pdf

Hutter, B.M. and O’Mahony, J, (2004) “The Role of Civil Society Organisations in Regulating Business”. London School of Economics (LSE) Discussion Paper number 28, September 2004. Published by the ESRC Centre for Analysis of Risk and Regulation, London, UK

Inventium (2015) “How do you balance customer and technology-led innovations?” 2 September 2015. Inventium website (accessed 14.11.16). Available at: http://www.inventium.com.au/how-do-you-balance-customer-and-technology-led-innovations/

Kolliarakis, G. and Ochs, A. (2016) “CSOs in security research”. Law and Internet Foundation (Bulgaria). SecurePART Policy Paper number 5, SecurePART project website. Available from: http://www.securepart.eu/download/securepart_pb-5160122155321.pdf

Kolliarakis, G. Ochs, A, Weber, R. Cornier, J, Sescu, M., Ionescu, D. and Botifoll, L. (2015) “Report on the collaborative links among CSOs”. 15 May 2015. Deliverable 3.2. SecurePART project, Project Number: 608039. Available from: http://www.securepart.eu/download/securepart-d_3_2_final151112162102.pdf

Ladd, J (2016, accessed 14.11.16) “The reporting system that sexual assault survivors want”. TED Talk, February 2016, Available from: https://www.ted.com/talks/jessica_ladd_the_reporting_system_that_sexual_assault_survivors_want

O’Brien, C. (accessed 28.11.16) Trojan T-Shirt Reaches Neo-Nazis. The Future of Ads. http://thefutureofads.com/trojan-t-shirt-reaches-neo-nazis

OEAW website (accessed 28.11.16) “Citizens’ Perspectives on Surveillance, Security and Privacy: Controversies, Alternatives and Solutions“. Joint conference of SurPRISE, PRISMS and PACT, 13th-14th November 2014, Vienna, Austria http://www.oeaw.ac.at/ita/fileadmin/redaktion/Veranstaltungen/konferenzen/jointconf/Programme-JointConference_Vienna2014_4.11.2014.pdf).

Orwell, G. (1949) “1984”. Secker & Warburg; London

SecurePart (2016) SecurePART project website. Available at: http://www.securepart.eu

SecurePART (2016) "SecurePART *Action Plan for Strengthening links between Civil Society Organisation and Security Research". Executive Summary*. Available from: http://www.securepart.eu/download/action-plan_06062016160606173554.pdf

SecurePART Final Conference (2016) "Strengthening the links between civil society organisations and security research", European and Economic Social Committee, Brussels, Belgium, 3 March 2016

SecurePART funding proposal (2013) "Increasing the Engagement of Civil Society in Security Research". EU 7th Framework Programme, Part B. Topic SEC-2013.7.3-1. Confidential funding consortium funding proposal submitted by Bantec, Spain

Technopolis Group (2016a) "Final Evaluation of Security Research Under the Seventh Framework Programme for Research, Technological Development and Demonstration". Full report available at: http://ec.europa.eu/dgs/home-affairs/e-library/documents/policies/security/reference-documents/docs/fp7_security_research_final_report_en.pdf

Technopolis Group (2016b) "Executive Summary". Final Evaluation of Security Research Under the Seventh Framework Programme for Research, Technological Development and Demonstration. Available at: http://ec.europa.eu/dgs/home-affairs/e-library/documents/policies/security/reference-documents/docs/fp7_security_research_final_report_summary_en.pdf

van Dijk, j, Tseloni, A. and Farrell, G. (2012) Introduction, in "The International Crime Drop. New Directions in Research". Crime Prevention and Security Management. (Eds) Jan van Dijk, Andromachi Tseloni and Graham Farrell, Palgrave Macmillan, United States

Von der Lippe, J, (2016) CSOs in Security Research. Austrian Red Cross. SecurePART Policy Paper number 10, SecurePART project website. Available from: http://www.securepart.eu/download/securepart_pb-10160224091249.pdf

International Perspectives of Crime Prevention 9
Contributions from the 10th Annual International Forum 2016 within the German Congress on Crime Prevention
Forum Verlag Godesberg GmbH 2017

Content