Rethinking the EU Security Research Programme

Submission by *Statewatch* in response to Section 4 ('Securing the citizen and the society') of the European Commission's consultation on an Industrial Policy for the Security Industry [1]

Introduction

The European Commission's concern for the ethics and societal impacts of its security research programme are welcome. It is imperative, however, that any changes bought about in FP7 or the next EU framework research programme offer more than 'cosmetic' compliance mechanisms. In this regard, we are very concerned that this consultation limits the scope of ethical concerns to matters related to personal data protection, creating a danger that other important societal impacts and ethical issues will be overlooked.

This will only fuel growing public concern about the development and implementation of 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 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 a more fundamental reappraisal is necessary.

In this submission we highlight five structural problems with the existing security research programme and recommend a number of changes that could produce a more balanced agenda – one that serves not just the needs of the security industry but those of democracy, proportionality, fundamental rights and the people of Europe.

1. **A confusion of the aims in the security research programme has resulted in a disproportionate focus on surveillance technology and coercive measures at the expense of European values and EU Treaty objectives**

As stated in the consultation, the EU security research programme has the twin aims of making people safer and establishing a strong internal market for security. These aims are not necessarily complementary. While technology clearly has an important role to play in enhancing European security, it is imperative that an already relatively secure Europe take steps to address the root causes of insecurity (at home and abroad) and begin to counterbalance the overwhelming focus on increasing security of the last decade with measures to restore civil liberties, preserve fundamental rights and enhance accountability. All of these initiatives could be addressed as part of a much broader 'human security' research agenda.

---

[1] This submission was prepared by Ben Hayes in May 2011. For more information about *Statewatch's* work on the European Security Research Programme see: http://www.statewatch.org/Targeted-issues/ESRP/security-research.html.

We are particularly concerned that the consequences of establishing a 'strong internal market for security' have not been properly thought through. Research programmes that seek to create 'competitive' Homeland Security industries inevitably favour policy outcomes that depend upon increased expenditure on security hardware and new-technologies. This in turn promotes the use of surveillance and a transfer of military technologies into the realm of civil security above other values and principles. The promotion of these technologies also inevitably relies upon the perpetuation of the sense of fear and insecurity that created the Homeland Security industry in the first place. These negative political forces can and have had a profoundly negative effect on democratic debate about EU security policies. There has, for example, been little in the way of critical public research and debate around the effectiveness and impact new security technologies.

According to the 'Review of security measures in the Research Framework Programme' commissioned by the European Parliament's Citizens' Rights and Constitutional Affairs' Policy Department and published in October 2010:

> a large proportion of [the] projects [funded under the ESRP] is dedicated to developing technologies of surveillance, to the detriment of a broader reflection on the impact of such technologies for citizens and persons concerned with the EU's security policies (page 8).[2]

Linking the EU security research programme to procurement, as suggested by the consultation, will exacerbate these problems and create a further danger that European security policy develops according to technological determinism instead of democratic debate. Research for the purposes of procurement falls outside the Treaty objectives of fostering knowledge and innovation and should only be undertaken as part of a fully accountable public policy programme. Procurement should thus be expressly excluded from the EU framework research programme 2013-2020.

It is equally important to prevent the security research programme being used for defence research, as suggested by the consultation. While the boundaries between defence and civil security technology appear ever more blurred, it is still relatively simple to distinguish between research that primarily serves the defence sector and research that primarily serves the needs of society. Defence research can and should therefore be expressly excluded from current and future security research programmes. There should be no structured cooperation between the security research programme and the European Defence Agency (EDA). If the EU wishes to fund military research outside the scope of the EDA agreement then this should be done through a separate defence cooperation initiative whose merits can be debated by the people of Europe and their elected representatives.

---

[2] Jeandesboz, J. & Ragazzi, F. (2010) *Review of security measures in the Research Framework Programme*. Brussels: European Parliament Directorate General for internal Policies, available at: http://www.statewatch.org/news/2010/nov/ep-review-security-research-programme.pdf.

2. The development of the security research programme has favoured the interests of the defence and security industries over the concerns of civil society and other stakeholders

The EU security research agenda has been strongly influenced by the representatives of corporations from the defence and security industries. The successive *ad hoc* advisory bodies established by the European Commission (the Group of Personalities, European Security Research Advisory Board and European Security Research and Innovation Forum) have all been dominated by industry stakeholders and perspectives.[3] According to the aforementioned 'Review of security measures in the Research Framework Programme' published in October 2010:

> EU security research and development activities have been mainly driven by a concern to bring together representatives from the ministries of Defence and Interior of the Member States and Associate countries, and representatives of major companies from the defence and security industries. In the process, representatives from civil society and parliamentarians, as well as bodies and organisations in charge of civil liberties and fundamental freedoms, including data protection authorities and fundamental rights bodies, have been largely sidestepped. **The outcome of this process is a dialogue that is limited in its scope, addressing security research through the concerns of security agencies and services and the industry, without taking into account the requirements flowing from the EU's internal area of freedom** [emphasis in original] (page 8).[4]

These concerns are reflected in this current consultation on 'an industrial policy for the security industry'. If the EU wishes to successfully address concerns about ethics and societal impacts in the next security research programme it is imperative that other stakeholders are given an equal voice. This will require new governance structures in which the concerns of the European Parliament, the European Data Protection Supervisor, the EU Fundamental Rights Agency, the European Group on Ethics in Science and New Technologies, civil society organisations and academia have equal weight in shaping the short and long-term priorities of the security research agenda.

3. Ethical considerations and societal impacts have been side-stepped in the drafting of the annual Calls for Proposals

The EU security research agenda is to a large extent dictated by the content of the annual Calls for Proposals. The process of deciding what to include and exclude in each Call is therefore crucial in terms of broader ethical considerations and societal impacts. The current process (in which Calls for Proposals are drafted by the European Commission on the basis of recommendations from the Security Advisory Group (SecAG) and then submitted for adoption by the Member States) lacks transparency and marginalises those stakeholders described above. The SecAG is dominated by defence and security companies that have profited most from the implementation of the security research programme to date, while expert EU agencies and civil society organisations are largely excluded. This arrangement has prevented sufficient deliberation of ethical issues and societal impacts.

In 2007 Franco Frattini, former European Commissioner for Justice and Home Affairs, stated:

---

[3] Hayes, B. (2009) *NeoConOpticon: the European Security Industrial Complex* (Transnational Institute/Statewatch), available at: http://www.statewatch.org/analyses/neoconopticon-report.pdf.

[4] See note 2, above.

> We need to listen to the technical experts to tell us what is technically feasible. Then we need to listen to experts on fundamental rights to see whether there are consequences of using these technologies that would put these rights in danger. It is only when we have considered all sides of the equation that we can find a balanced response.[5]

These minimum standards must now be implemented at the programmatic level. All Calls for Proposals in the security research field should first be subject to an ethical review that pays full regard to the potential societal impacts of using the technologies encouraged by the underlying R&D agenda. Any important ethical issues and/or societal impacts raised by such a review must then be fully incorporated into the Call for Proposals, both as an integrated part of the R&D agenda and through dedicated resources for research and analysis that address specific concerns.

4. Ethics and societal impacts have been 'pigeon-holed' by the current security research programme

Where ethical issues and societal impacts have been addressed by earlier Calls for Proposals in the area of security research, this has taken the form as stand-alone research projects that have had little bearing on the broader EU R&D agenda – not least because the findings have been largely ignored by the architects and beneficiaries of the security research programme. Unless ethics and societal impacts are taken more seriously and fully integrated into all EU-funded research projects then widely held concerns about many security technologies will have continue to be sidestepped in practice.

The current ethical guidelines for EU-funded security research are inadequate. They are derived from ethical issues that have arisen in the field of bio-medical research and only further address privacy and data protection. Here the rules are much less concerned about the right to privacy *per se* (freedom from undue interference in one's personal life) than consent and compliance with limited EC data protection rules.

It is imperative that the process for evaluating and funding proposals is changed to ensure that security research proposals address ethical issues and societal impacts in a much more coherent manner. One the one hand this will require significant expansion of the existing ethical guidelines to address a much broader range of issues pertaining to fundamental rights and the societal impacts of security technologies and policies. On the other hand it will require applicants to address these issues in their proposals and then integrate them into their projects at every stage. Proposals that do not adequately address these issues should not receive EU funding. Proposals that raise substantive concerns should be subject to robust and ongoing scrutiny by supervisory bodies.

5. The EU security research programme has failed to address the broader challenges posed by securitisation

While much has been done in the attempt to enhance European security over the last decade, critical social scientists have identified a number of pressing concerns about the securitisation and militarisation of European societies. These largely negative societal impacts include increased public

---

[5] Frattini, F. (2007) *'Security by design', Homeland Security Europe*, based on a speech by Commissioner Frattini to the EU Security Research Conference in Berlin, 26 March 2007, available at: http://www.homelandsecurityeu.com/currentissue/article.asp?art=271247&issue=219.

expenditure on security at the expense of other public goods, the outsourcing of surveillance to a growing private security industry, a focus on 'threats' rather than root causes, a shift from reactive to proactive policing, excessive criminalisation, a clampdown on civil liberties, the targeting of 'suspect communities', the expansion of executive powers and security controls, the emergence of new networked systems of law enforcement and control, and the difficulty in maintaining liberal democratic 'checks and balances' in these new security landscapes. The security research programme has fuelled concerns in all these areas without properly considering the implications for future European generations.

The growth of the European Homeland Security industry and the dominance of the sector by defence companies pose additional problems in terms of regulation and accountability insofar as they encourage the transfer of military logics into the realm of civil security and promise to endow less democratic and authoritarian states with powerful security apparatuses. The ongoing events of the 'Arab Spring', in which a number of regimes have used arms and security equipment made in the EU to brutally repress their own people, points toward an urgent reflection as to how to ensure that various technologies that have been supported by the EU security research programme do not end-up in the hands of governments with poor human rights records. Instead of the "Opening up of international markets for security products by making full use of the EU's trade policy strategy", as proposed in the Consultation, the EU should instead be focussing on how to link its trade policies to a conflict prevention and human security agenda that will enhance global security and prevent human rights abuses in the longer-term.

Finally, it is imperative in an era of austerity that all security expenditure, including EU R&D funding, is subject to meaningful audit to assess both effectiveness and 'value-for-money'. The twin obsessions with security and technology have been ceaselessly exploited over the past decade to justify increased public expenditure. If an incident occurs, it is a reason for spending more on security; If no incident occurs, it justifies what is already being spent. This is a false economy that stifles rational thought and critical evaluation of new security systems. Current and future security research programmes must therefore include rigorous auditing mechanisms that assess both the cost-effectiveness and broader socio-political context of the research it has funded. An adequately resourced body with a sufficient degree of independence should be tasked with conducting such evaluations.

6. Summary of recommendations

(i)   The EU should radically reassess the priorities of European Security Research Programme, limit the funds spent on security technology and dedicate far greater resources to addressing root causes and conflict prevention. This will entail a shift away from the current, overly-simplistic focus on security threats to a broader consideration of how to address international security problems through a range of different policy options.

(ii)   The European Commission should resist plans to link security research to procurement and/or military research in the next EU framework research programmes. Should the EU wish to pursue these goals, it must do so using dedicated policy instruments relating to procurement and defence cooperation instead of the EU research policy framework.

(iii)   The development and implementation of the security research programme must be opened-up to a full range of stakeholders, including civil society, at every stage of the decision-making process.

(iv)   All Calls for Proposals and all proposed projects in the area of security research must be subject to a significantly expanded ethical review. This review must extend beyond the narrow confines of privacy and data protection take into account the broader societal impacts of the underlying security R&D agenda. Calls and project proposals that raise substantial ethical and/or societal impact concerns must be subject to enhanced scrutiny and control.

(v)   The EU Security Research Programme should be brought under the auspices of a new Human Security 'Grand Challenge' overseen by DG Research. This could help revitalise EU policies in the area of international security, human rights, non-discrimination, social inclusion, conflict prevention, conflict resolution, security sector reform, accountability and the rule of law. A Human Security Grand Challenge would also impose a normative model for European research and innovation that emphasises scientific openness to the world and the free circulation of knowledge in place of the narrow state-corporate security agenda that has emerged under the existing FP7 programme.[6]

(vi)   The development of Europe's Homeland Security industries must be accompanied by new regulatory mechanisms. At a minimum these mechanisms must address the problems of developing security technologies that implicitly threaten universal human rights and the export of these technologies to repressive and authoritarian regimes.

(vii)   EU expenditure on security research must be accompanied by rigorous audit mechanisms that subject the security R&D agenda to meaningful critical assessment. If the EU is to ensure value for money across its technology platforms and innovation programmes then it must establish oversight mechanisms that can identify problematic issues such as research bias, conflict of interests, excessive cost, potential harms and other matters that have been left unaddressed by the current EU framework research programme.

---

[6] The proposal for a Human Security Grand Challenge is included in policy options proposed by the EU-funded SANDERA project on the 'Future Impact of Security and Defence Policies on the European Research Area'. The EU's own criteria for setting a Grand Challenge are 'attractiveness-relevance', 'attractiveness-research' and 'feasibility'. As noted by the SANDERA project: 'The first and second sets of criteria appear to be fulfilled by human security. Human security would appear to be relevant, with potential European added value and in support of EU policies (not least the European Security Strategy). Equally, it would appear to meet the second criterion since there is a potentially strong research component. With regard to the third criterion, a human security Grand Challenge would also appear to be feasible. It seems likely that it would appeal to the research community and may well capture public imagination'. For more information see http://www.sandera.net/.