# Consultation on an Industrial Policy for the Security Industry

## 1. Respondent profile

### 1.1. Name
Martina Weitsch

### 1.2. Please provide an email adress where we can contact you
mweitsch@qcea.org

| 1.3. You are/you represent | Non governmental organisation |
|---|---|

### 1.4. Name of Organisation
Quaker Council for European Affairs (ID on Commission Register of Interests: 3960234639-24)

### 1.5. Job title
Head of Office

### 1.6. Day-time phone number
+32 2 234 3064

| 1.7. In which country are you/is your organisation based? Please specify | BE – Belgium |
|---|---|

### 1.8. What is your/your organisation's main sector of activity?
We believe that all people can live in peace and therefore advocate non-military responses to conflict and peacebuilding and for conflict prevention in foreign relations. We also work on human rights, energy security and economic justice.

### 1.9 What security solutions does your company produce/offer?

We do not produce or offer 'security solutions'; we offer a perspective on security that starts with the fundamental belief in the equality of all people and the need to live globally in community so that the luxuries of some do not come at the expense of the misery of many.

## 2. Market Fragmentation

### 2.1.1. Certification/conformity assessment procedures

#### *Problem definition*

| Do you agree that the lack of harmonised certification/conformity assessment procedures for security technologies affects the market fragmentation?<br><br>(ranking from 1 do not agree at all to 4 agree very much) | Do not know |
|---|---|

### 2.1.2. Please indicate on a level of 1 to 4 which of the policy options described below do you think is most effective and realistic to reduce market

**fragmentation:**

| Option 1: No change - certification/conformity assessment procedures will continue to be regulated by national systems. | Do not know |
| --- | --- |

| Option 2: EU wide harmonised certification/conformity assessment procedures covering all (or at least as many as technically possible) security products | Do not know |
| --- | --- |

| Option 3: Step by step: certification/conformity assessment procedures focused on certain priority areas or priority technologies where there is a clear EU added value. | Do not know |
| --- | --- |

Other option

(please describe - upload of additional documentation is possible)

We believe that it is far more important to address the questions relating to the ethical issues raised by security research than the question of market fragmentation. Some degree of market fragmentation can contribute to a more differentiated approach to what is acceptable in ethical terms and to more open debate about appropriate solutions. This does require informed public participation which in our view should be an important component in any EU-funded security research projects.

2.1.3. Could you please specify for which products, technologies and/or systems you experienced problems due to differing national certification/ conformity assessment procedures?

## 2.2.1 Standardisation

| Do you agree that the lack of EU wide standards for security affects the market fragmentation? (ranking from 1 do not agree at all to 4 agree very much) | Do not know |
| --- | --- |

## 2.2.2. Please indicate on a level of 1 to 4 which of the policy options described below do you think is most effective and realistic to reduce market fragmentation:

| Option 1: No change: continue the ad-hoc, piece meal approach whereby the Commission mandates the ESO's to develop EU-wide standards based on immediate needs. In parallel industry develops on its own initiative EU-wide standards. | Do not know |
| --- | --- |

| Option 2: Industry driven - the Commission would stop mandating the ESOs to develop standards, but would leave this process entirely to industry | Do not know |
|---|---|
| Option 3: Step-by-step end-user driven standardisation based on a careful identification of existing, national, European and international standards, via Commission mandates to ESO's | Do not know |

Other option


(please describe - upload of additional documentation is possible)

We do believe that an industry-driven approach will have a strong effect, but in our view a very negative one. The EU's approach to security research should not be driven by the impetus of security organizations to sell more hardware; it should be driven by what citizens actually see as priorities within the parameters of ethics – including but not limited to concerns about privacy. In other words, for us, this is not the most relevant approach to reviewing the security research programme.

## 2.3. Follow up question on market fragmentation I


**Could you please specify for which products /technologies and/or systems would you consider EU-wide standards most needed to overcome market fragmentation (upload of additional documentation is possible)?**

We do not believe that market fragmentation is the main issue; the main issue is what is ethically defensible. In our view there should be a focus on developing relevant ethical standards for all security research (including nanotechnology and space research); this must go beyond issues of privacy. To achieve this, each project funded under these programmes should have a mandatory ethics component involving appropriate social scientists and a degree of citizen participation and consultation.

| **2.4. Follow up question on market fragmentation II**<br><br>Do you consider it useful to include in a possible certification assessment procedure not only products, but also systems (a number of interconnected technologies) and processes (multiple technologies + related services)? (Upload of additional documentation is possible) | Do not know |
|---|---|

## 2.5. Further suggestions


**Do you recommend any additional measures that would effectively tackle market fragmentation (upload of additional documentation is possible)?**

| 2.6. Subsidiarity principle<br><br>Do you consider that action by the EU would be necessary to reduce the market fragmentation? | Do not know |
|---|---|

## 3. Fragile industrial base

### 3.1.1. Could you please provide your views on a level of 1 to 4 on the fragility of the industrial base:

| Do you agree that the EU security industrial base is fragile? | 1 |
|---|---|

### 3.1.2. Could you please elaborate on what this fragility of the industrial base consists of in your view:

| Fragile in terms of third country competition | 2 |
|---|---|
| Fragile in terms of development of state of the art technologies | 2 |
| Fragile in terms of access to finance | 2 |
| Fragile in terms of dependency from the primes | Do not know |

| Other option<br><br>(please describe - upload of additional documentation is possible) |
|---|
| |

### 3.2. Pre Commercial Procurement

### Please indicate on a level of 1 to 4 which of the policy options described below do you think is most effective and realistic to reduce market fragmentation:

| Option 1: No change Pre-commercial Procurement in the area of security would be solely done on a national level | Do not know |
|---|---|
| Option 2: Pre-commercial procurement activities would be carried out in FP8 but without specific financing instruments | Do not know |
| Option 3: A focused pre-commercial procurement scheme being built up via the possible future FP8 and/or CIPII funding. | Do not know |

| Other option |
| --- |
| (please describe - upload of additional documentation is possible) |
| Our main concern with the security research programme is not market fragmentation; it is the ethics dimension of the programme. Pre-commercial procurement suggests that there is some kind of public buy-in to technologies and approaches that have not been fully developed and that have not been tested either in terms of potential harm or in terms of their acceptability to the public. Any approach that may commit public authorities to procuring in this way is contrary to an ethical security policy. |

## 3.3. Defence and Security Procurement

**Please indicate on a level of 1 to 4 which of the policy options described below do you think is most effective and realistic to reduce market fragmentation:**

| Option 1: No change – The Defence Procurement Directive will now provide a clear and sufficient framework to contribute effectively to reducing market fragmentation. | Do not know |
| --- | --- |

| Option 2: Encourage security customers to pool their investment resources in order to achieve interoperability and economies of scale. | Do not know |
| --- | --- |

| Other option |
| --- |
| (please describe - upload of additional documentation is possible) |
| We are concerned that the phrasing of option 1 indicates that security research is seen as defence research. We believe there should be a differentiation on an ethical basis and this should be reflected in the way the security research component of FP8 is framed. The move towards military research funded from EU research budgets which is implicit in the formulation of this option is one we strongly advocate against. |

## 3.4. Synergies between civil and defence technologies

**Please indicate on a level of 1 to 4 which of the policy options described below do you think is most effective and realistic to reduce market fragmentation:**

| Option 1: No change - the Commission would | Do not know |
| --- | --- |

| | |
|---|---|
| continue to coordinate research activities between FP7 and EDA on an ad-hoc basis | |
| Option 2: Strengthening synergies between civilian and defence technologies in a step by step approach via more upstream coordination at the level of capability development and more downstream coordination at the level of development of standards | Do not know |
| Option 3: In addition to option 2, this option would go beyond coordinated research activities by establishing a dedicated civil-military research programme as part of FP8 | Do not know |

Other (please describe - upload of additional documentation is possible)

For us it is not a question of the effect any of these steps may have; we are strongly opposed to any part of FP8 opening the door to military research in any form. There should be more emphasis on researching the root causes of security problems, like terrorism, and socially acceptable and ethical responses to this which should not be primarily or even tangentially military in nature. Security threats are predominantly criminal rather than military in nature and should be addressed in that way.

## 3.5. International markets

**Please indicate on a level of 1 to 4 which of the policy options described above  do you think is most effective and realistic to reduce market fragmentation:**

| | |
|---|---|
| Option 1: No change - the EU would not undertake any specific activities to encourage access to third markets for the EU security industry | Do not know |
| Option 2: Opening up of international markets for security products by making full use of the EU's trade policy strategy. | Do not know |
| Option 3:In addition to option 2 -  the Commission would aim at fostering the adoption of joint or common approaches at international level, notably in the area of standards via the International Standardisation Organisation. The approach would also provide an opportunity to raise the visibility of the European security industry around the world. | Do not know |

Other option

(please describe - upload of additional documentation is possible)

For us it is not a question of the effect any of these steps might have; we are strongly opposed to entering into security cooperation with non-EU actors without significant consideration of their security policies vis-à-vis their own populations or populations over which they exercise control. An ethical approach to security requires the respect at all times for human rights and democratic governance and this must be guaranteed both for EU actors and associated countries.

## 3.6. Third party limited liability protection

## Please indicate on a level of 1 to 4 which of the policy options described above do you think is most effective and realistic to address the issue of third party limited liability protection:

| | |
|---|---|
| Option 1: No change - under this option the EU would not get involved in Third Party Liability issues | 1 |
| Option 2: Introducing harmonised rules at EU level on Third Party Liability Limitations for security products/processes/systems in case of a terrorist incident. Under this option the EU would define under which circumstances and conditions companies/system operators could invoke Third Party Liability Limitation. The EU would also define the minimum or maximum financial compensation up to which companies/system operators would be liable for | 4 |
| Option 3: Encouraging Member States to introduce such legislation at national level with the Commission as guardian of the Treaty ensuring that such a decentralised approach does not lead to internal market barriers. Under this option, the Commission would set out guidelines to help Member States in setting up Third Party Liability Limitation schemes that would not be contradictory between different Member States, thus leading to internal market barriers | 2 |

Other option

(please describe - upload of additional documentation is possible)

It is essential that there is as little wriggle room as possible for security technology suppliers when things go wrong. People affected by such technologies when they do go wrong and do harm should have recourse to those whose technology is at fault and this should include both the public authorities and private organisations procuring such systems and the manufacturers of such systems. Minimal wriggle room would also deter industry and end users from taking unacceptable and unethical risks.

## 3.7. Follow up question on third party limited liability market fragmentation

**Could you please specify whether you experienced problems regarding third party liability on a national and/or EU wide level? (Upload of additional documentation is possible)**

---

**3.8. Further suggestions**

**Do you recommend any additional measures that would effectively strengthen the security base in the EU (Upload of additional documentation is possible)?**

FP8 should widen the ethics article included in FP7 beyond bio-ethics to include the issues raised by nanotechnology, security and space research. Given the complexity of this, there should be an advisory body on ethics as a formal part of the FP8 management structure and a requirement to include an assessment of the ethical implications of each research project within the project design. This would require the obligatory participation of suitably expert social scientists in each such project.

| **3.9. Subsidiarity principle**<br><br>**Do you consider that action by the EU would be necessary to reinforce the industrial base?** | Yes |
|---|---|

## 4. Securing the citizen and the society

### 4.1.1. Problem definition

| Do you agree with the problem definition, that security products need to be privacy compliant from the development to the production?<br><br>(ranking from 1 do not agree at all to 4 agree very much) | 4 |
|---|---|

### 4.1.2. Which option, on a level of 1 to 4 do you think is effective and realistic to ensure that the ethical/societal dimension of security is introduced in an industrial policy for the security sector?

| Option 1: No change - privacy by design would remain a voluntary effort for industry with no EU wide guidelines and/or requirements | 1 |
|---|---|

| | |
|---|---|
| Option 2: A voluntary certification/conformity assessment system. Under this option the economic operator wishing to have his product/process/system certified for being "privacy by design" fit, would have to fulfil a set of requirements defined by the EU. However, the certification/conformity assessment itself would remain voluntary. | 1 |

| | |
|---|---|
| Option 3: In addition to option 2 – the certification certification/conformity assessment would be mandatory | 3 |

| |
|---|
| Other option

(please describe - upload of additional documentation is possible) |
| Ethical/societal implications of security research are not limited to privacy issues. There are for example issues such as dual use goods, the militarisation of security, the ethics of end users (not exclusively in third countries) and reference to human rights and democratic governance in security policy. Beyond that, there is an issue about the privatisation of security with the easier access to cheaper but intrusive technology. Ethics must be an intrinsic part of programme and project design. |

| | |
|---|---|
| **4.2 Certification procedures**<br><br>**Do you believe it to be useful to merge a possible ethical certification procedure as detailed in point 4.1. should be with the certification procedures outlined in point 2.1, instead of having two separate certification procedures?** | Not useful |

| |
|---|
| ## 4.3. Research on Privacy compliant technologies

**Which option, on a level of 1 to 4 do you think is effective and realistic to ensure that the ethical/societal dimension of security is introduced in an industrial policy for the security sector?:** |

| | |
|---|---|
| Option 1: No change - Through targeted research projects in the Security Theme of the FP aimed at developing "privacy by design" technologies. These technologies could then be applied in future security products, processes or systems. | 1 |

| | |
|---|---|
| Option 2: Making the privacy compliance a mandatory evaluation criteria for all technology related research proposals | 4 |

under the Security Theme of the FP. Under this option, the EU would make it mandatory to address privacy by design in all technology related research proposals of the Security Theme of the FP.

Other option

(please describe - upload of additional documentation is possible)

Ethical/societal implications of security research are not limited to privacy issues. For example issues such as dual use goods, the militarisation of security, the ethics of end users (not exclusively in third countries), human rights and democratic governance in security policy and the privatisation of security with the easier access to cheaper but intrusive technology are all critical concerns. Ethics compliance must be mandatory and much wider than privacy by design.

**4.4 Further suggestions**

Do you recommend any additional/other option that would effectively reinforce the ethical/societal dimension of security in the envisaged industrial policy for the security sector (upload of additional documents is possible)?

*Please elaborate*

## 5. Final questions

**5.1 Are you aware of any initiatives in your country that have one of the above goals in mind (upload of documentation is possible)**

**a) Reducing market fragmentation**

**5.1. b) Strengthening the industrial base.**

5.1. c) **Introducing the ethical/societal dimension in security technologies.**

## Meta Informations

Creation date

12-05-2011

Last update date

User name

null

Case Number

165357401411013211

| Invitation Ref. |
| --- |
| |

| Status |
| --- |
| N |

| Language |
| --- |
| en |