Minutes

5th Meeting of the Horizon 2020 Protection and Security Advisory Group (E03010)

January 24, 2017, Brussels

1. Approval of the agenda and of the minutes of previous meeting

The draft agenda and the minutes of the previous meeting were approved.

2. Nature of the meeting

The meeting was non-public. Two former PASAG members, whose membership expired end of 2016, were invited as experts to report on their work until the end of 2016.

3. Opening (PASAG Chair)

Tasks for this meeting comprise commenting on working group papers (following up with feedback and comments over the coming days is expected).

Changes in the PASAG membership, due to memberships ending end of 2016 and withdrawals were notified to colleagues.

Overall there is a need for members of working groups to be more proactive in contributing to the reports and it needs to be made sure members volunteering can commit time and effort to the work. Otherwise it is difficult for the lead on the group to make sure the substantial amount of work needed, is completed. An early outline brief is useful to stimulate contributions, even a set of ideas or one-pager noting the subjects to be addressed.

Because meetings of the PASAG are few, it needs to be ensured that working together remotely, is more agile and functional and any suggestions on how to do that are welcome.

The European Commission highlighted the importance of the reports by the PASAG in addressing policy issues and the agreement to publish them over the course of the year in an edited format. The audience for the working group reports will be the existing EU security community.

4. List of points discussed

4.1. Finalisation of reports from Working Groups (WG Chairs Presenting and Discussion)

4.1.1. WG1 (Leveraging R&D&I to develop capability and enhance security industry sub-sectors)

The former WG Chair (and PASAG member until end of 2016) reported: There was a long discussion at the previous meeting so the main areas have been taken into account in the report. There is more on Cyber and ICT in text. Main addition on experimentation and cluster issues at the end.

Discussion raised issue of PPP and how this could be effective over a year or two as results would not be seen until after that. The European Commission explained that activities could be launched that go into the next programme and while the exact content of that programme could not be predicted, it was likely there would be relevant areas of focus. Suggestion fine and up to Commission to find appropriate approach.

The issue of testbeds was raised and whether these had application beyond cyber. Testbeds are useful in the Cyber environment because they offer the opportunity to test new technologies in a controlled and isolated environment before certification and release. For SMEs they are particularly useful as they would allow cost-effective testing that SMEs cannot undertake on their own. Most customers in the market currently prefer buying Cyber solutions from big vendors that can provide the required assurance. ENISA does not currently have this capability but could be a potential provider of independent assurance and validation capability.

The former Chair of the WG explained that experimentation and validation had been introduced as a general proposition, because of the value they carry in the innovation process. The European Commission indicated that PASAG's suggestion that part of the infrastructure of research should include testbeds, experimentation, and validation, is welcome. Clearly, there is a significant overall investment across the EU in test centres and validation laboratories. Rather than recommending new facilities, it would be more appropriate to indicate how best to use existing capacity in a more coordinated way. It was also suggested that sustainable solutions be introduced as a focus and that concrete recommendations on sustainability be included.

The European Commission explained that there are regional clusters helping share expensive infrastructures and prototype testing and that this type of approach could be replicated. A network of existing, mostly regional, clusters/facilities could be recommended to ensure harmonisation and sharing of facilities. If solution providers require expensive certification this could provide a pre-route before that formal process.

The PASAG Chair has agreed to assist in completing the report with the observations made at the meeting and distributing a draft to the PASAG membership for final comments in the next days, prior final release.

4.1.2. WG2 (Combining existing H2020 pre-procurement tools, resources from EU programmes beyond H2020 and from EU Agencies in the field of security)

The WG Chair reported: Goal is to make innovation happen – bring results into market success. Possibility of IP free to SMEs? Need to bridge the gap and overcome the valley of death (lack of investment in taking new ideas to market) and incentivise research entities to get knowledge out into the market.

The discussion raised the issue of pre-procurement and The European Commission said the intention in 2018 was to call for PCPs without being outcome specific, to enable, for instance, the development of prototypes and fund other pre-production activities. Users must be involved in such applications, it was noted. There could also be a topic in the 2018-20 with support for PPI, which could offer an additional entry point. It will very much depend on the proposed level of innovation and market conditions on whether the Commission would support it. There was some concern that the support at 30% of total investment may not be attractive enough, but it was also pointed out that the rationale for investment is not only the availability of finance.

There was an extensive discussion within the Group, with different views expressed, on IPR, including:

- SMEs and start-ups have difficulty with the long and expensive process of negotiating access to IPR with Academia and research institutions. EC funded projects should provide for a framework that sets the terms of the IPR agreements to expedite and simplify licencing arrangements. JRC could be relevant here rather than producing new structures.
- IPR should be an element of the pre-procurement process with any consortium owning it.

- A debate within research communities and start-up sector about ‘open innovation’, ie. the open access to IPR generated by Academia and research institutes as a stimulus to innovation and economic growth, and its relative benefits and disadvantages. In this regard, an approach may include testing open innovation in some specific technology/solution areas.
- Security has the added constraint that its technologies have security implications which may limit the opportunity for access, making open access even more difficult.
- Research institutes in several cases are also providers of the capability solution that compete with other providers in the commercial market. This makes it more difficult to attract their engagement with the prospect that the resulting IPR may be accessible for free or at low cost.
- EC funding cannot discriminate between participants, favouring some (SMEs, start-ups) over others.
- Additionally, in some cases, IPR resides with Government entities, which complicates access.

The WG was encouraged to include in the report some of the comments from the PASAG meeting and to examine other innovation models, particularly the DARPA/ARPA model in the US, and add reference to this in the report identifying what benefits they could bring the EU environment and what options there may be to adopt something similar to existing institutional arrangements.

4.1.3. WG4 (Achieving synergies between security and information-related fundamental rights (IRFR) in a digital intensive environment)

The WG Chair reported: The report is work in progress and needs further development, including further analysis of the enforcement and intelligence agencies requirements that may impact the relationship between privacy and security, among other areas. It is anticipated that new members joining the PASAG from those communities will be able to offer contributions in these areas. Additionally, ENLETS could provide similar contributions.

Industry 4.0 (Internet of Things) is another dimension that requires further development, because of the potential important implications for individual privacy and security and the lack of any regulatory framework or guidance for industry that is developing these capabilities. The report also does not specifically address the implication and risks of end-to -end encryption. Where views differ, the report should reflect this. Additional comments submitted need to be incorporated as well.

The discussion covered several areas including:

- Privacy by design is referred to indirectly in a number of areas of the report, but lacks clarity as a concept, which needs further analysis, particularly as recent European legislation incorporates this language and therefore there needs to be an understanding how it applies and what does it refer to. The extent to which privacy by design is a universal concept was raised—it may be better understood as ‘situation specific’.
- The bulk surveillance debate and whether it can be legally or ethically justified, both in terms of privacy and security. The associated issue of proportionality should be subject of further review.
- Technical solutions are not the only way to address the issue, but other areas including legislation, organisational should be considered.
- The need to balance the focus in the report not just on the encroachment of the State on the privacy of the individual but also by businesses which increasingly exploit data collected from citizens to further their market strategies.

It was agreed that the necessary time should be taken to develop this report along the above lines. Teleconference meetings will be considered to assist in this process. One member referred to a programme being developed on social media in Sweden on which input will be provided.

4.1.4. WG5 (Validating innovative security solutions through processes to take account of practitioners' requirements and citizens' expectations)

The WG Chair welcomed feedback on draft report so far. Importance of practitioners being involved at every stage including setting-up of projects and the recognition that some may be users and others not; and that they need to clearly appreciate the overall value of the project and the value to themselves of being involved, given their other heavy commitments. Organisations representing practitioners should work with the EC to enable their input into programmes in the definition phase. Solutions transferred from defence contexts may not suit the needs of civil practitioners. Innovation might be in products and working practices as well as in policy, not just technology. The project review process must take account of practitioner priorities for funding.

The European Commission suggested that there is much greater engagement by practitioners in current calls including five practitioner-led network projects, and therefore the report should start analysing the experience gained from this involvement. The EU-funded project to engage CSOs in EU security research (SecurePART) was specifically mentioned, in this respect. Additionally, practitioners can now be full members and project leaders. First outcomes should be available in the summer and it may be worthwhile for the report to delay publication until some of these experiences can be reviewed. The European Commission also highlighted the inclusion of open calls, where topics are identified by funding applicants —this was described as a 'bottom up approach'.

Discussion included:

- Need to be aware of different funding conditions of police forces across Europe with some forces being left out of these developments, as well as the possible need for training or capacity-building for meaningful engagement.
- Problems of time commitment for end-users involved in projects and lack of professional recognition (in the hierarchy) of the value of such involvement, discourages engagement.
- Practitioners may have a sense of projects being too narrow in focus, and often be looking for an international perspective (rather than national orientation relevant to many practitioners).
- Cost element of practitioner participation is important and in some cases, may be too high for their budgets – examples include fielding of expensive practitioner assets for trials.
- Training courses may be needed for end-users to explain how they should participate, what is the added value for them, and some support for them in terms of cost, etc.
- Industry very much wants and support practitioner involvement in security projects—it was suggested that this should be communicated more strongly in WG5's report.
- The importance of early involvement by practitioners in project proposals and of dialogue was highlighted. This is time-consuming and practitioners may withdraw from the process due to other commitments.
- Practitioners become frustrated if project proposals oriented towards their requirements seem not to be valued by reviewers of EU security funding proposals.

The other element of the report addresses citizens' expectations, where there is a need to recognise they are not always users, while there is a growing tendency for projects to consider the relevance of citizens' expectations. Solutions of proven value that reduce security risk, improve feelings of security, and address values including human rights. Civil Society Organisations (CSOs) are of potential real value, including in testing solutions and identifying which ones can work, engagement with them around complex problems, and importance of involving CSOs in real projects. Discussion raised the point that CSOs may not be neutral participants so this needs to be considered.

It was agreed that the WG Chair would contact HOME-B.4 regarding the actions and results related to greater practitioner participation in EU-funded security projects.

Issuance of the report would await outcomes of first practitioner involved projects in the summer.

4.1.5. WG6 (Dual-use R&D&I - the Civilian Perspective)

The former WG Chair (and PASAG member until end of 2016) reported: A new title for this WG is proposed. Areas of focus include: contrast between long military and short commercial planning processes and resulting problems of alignment across these sectors; high costs of defence products; proposals for PCP/clusters could identify areas of common interest (the European Commission noted that this is an important area and a current call could feed into this).

The draft report needs more input which will need to be provided over the next few months. The area is particularly important given the EC engagement on a future defence technology funding programme and the associated need to ensure there is no duplication with programmes funding technologies for security rather, where appropriate, leveraging dual-use opportunities.

4.2. Horizon 2020 Secure Societies Work Programme 2018-2020: Next steps

The European Commission reported on the preparations of the next Work Programme.

For the Horizon 2020 **Societal Challenge 7** (Secure Societies) Work-Programme 2018-20, PASAG will be invited to make suggestions for the impact section when first draft is ready in mid-March. Members will be asked to comment on the impact section when the final draft is ready in June.

4.3. PASAG interaction with other Horizon 2020 Advisory Groups

The European Commission reported about the Focus Area - Boosting the effectiveness of the Security Programme. Aim to have a set of common principles that will operate across the DGs and this is now under discussion. New Commissioner has responsibility for security across the DGs. While all budget decisions will stay with the DGs there is the potential to share principles, co-ordinate calls better and prioritise topics. A common pool of experts could be used in evaluation.

PASAG members supported idea of chair of PASAG meeting with other Advisory Group chairs, two or three in the first instance, to identify important topics. This could then be followed up with meetings of members of the different Advisory Group interested in a given topic. In addition to general areas of shared focus there would be overlapping topics to look at.

4.4. Other

- Plan to issue **PASAG documents** in **published** versions – initially Vision document and several working group reports as they are finalised – to be made available at the Security Research event and other conferences for a programme committee, industry and research audience.
- An up to date list of **current members of PASAG** was distributed and it was explained that membership is being renewed for about a quarter of the group at a time to ensure continuity. A list of nine potential new members have been approved by the Director General including practitioners covering customs, intelligence, and utilities, and members of CSOs recognised as interlocutors in the EP.

5. Next meeting

Next PASAG meeting proposed for Wednesday 28 June 2017.

6. List of Participants

A. de Benedictis (Chair), G. Youngs (V. Chair and Rapporteur), J. A. Cannataci, C. Davey, C. Gaertner, K. Keus, H. Lindberg, F. Martinelli, R. Riesco Granadino, A. Spronska.