Group of Chief Scientific Advisors

Cybersecurity in the European Digital Single Market

Stakeholder Meeting Report

Scientific Advice Mechanism

13 February 2017, Brussels

Cybersecurity in the European Single Market

Stakeholder Meeting hosted by the High Level Group (HLG) of Scientific Advisors of the European Commission's Scientific Advice Mechanism (SAM)

13 February 2017, Brussels

MEETING REPORT[1]

The meeting aimed to present the SAM HLG's draft findings to stakeholders - civil society, consumer organisations, businesses, as well as some policy representatives - and receive feedback. Around thirty stakeholder representatives were invited and took part. Following presentations by members of the SAM High Level Group, the floor was opened to collect reactions, comments and questions from the stakeholders.

On the whole, the discussion revealed agreement with the draft findings presented. No specific disagreements or concerns were voiced but rather many helpful suggestions and remarks were given. One overriding message was a need for clarity in presenting the recommendations regarding their intended relevance for going "beyond" the current EU cybersecurity policy agenda.

The main points which were raised in the discussion were as follows:

- A number of stakeholders stressed that in order for Europe to compete globally in cybersecurity much more investment in basic/ fundamental R&D is needed than is currently the case, in addition to the investments made in more applied ICT R&D such as highperformance computing, etc.

- A number of stakeholders expressed the view that while the aquis so far goes in the right direction much more is needed to protect privacy, to cater adequately for profiling concerns, opt-in versus optout questions, data minimisation, etc. and in the process to impact upon a fast-moving target. This includes policy actions to promote sharing, cooperation, training, a fit-for-purpose ENISA-type capability and so on. It was also pointed out that profiling can be beneficial and desirable to the service user and it can also play a role in increasing cybersecurity as well as provoking concerns.

- It was stated also by a number of stakeholders that the long lead time and a de minimis harmonization approach for EU legislation (e.g. NIS) is incompatible with the

[1] See meeting agenda and list of participants at the end this document

rate of change in and the ambition required for the CS area. The importance of information sharing between not just Member States but also with the private sector was stressed by many stakeholders.

- There was a strong endorsement of the SAM HLG's emphasis on training and in particular the need to increase technical expertise in relevant public authorities and oversight bodies bringing it up to a par with legal expertise which currently dominates.

- Emphases on fundamental rights and transparency were welcome by many stakeholders, particularly in so far as they inter alia help to eliminate inegalitarian and discriminatory practices built into algorithms ACM's Principles for Algorithmic Transparency and Accountability released in January 2017 were cited in this regard.

- Regarding software vulnerabilities, it was pointed out that there are new agile models that involve multiple releases.

- Some stakeholders pointed out that "Duty of Care" regarding followup patching/ repair requires reciprocation so that producers are not held legally responsible for costs resulting from failure on the part of the client/ user to take the repair on board.

- A number of participants spoke in favour of developing European technical and business capabilities for strategic reasons linked to trust, lessening foreign dependency, etc. - analagous to Gallileo visà-vis GPS, etc. Protectionism should be avoided as well as anything that would limit access to the best available technologies and skills.

- European participation in the setting of global (ISO-type) standards was deemed to be most desirable.

- Legal reporting obligations of cybersecurity incidents under different pieces of legislation and to different public authorities was deemed to be a heavy burden which could possibly be replaced by a more one-stop-shop approach, according to some views of the stakeholder community.

Overall, the meeting confirmed that the areas the SAM HLG is covering with the Opinion are of much interest to the stakeholder community. The chair of the SAM HLG and rapporteur for the topic Rolf Heuer thanked all participants for their contribution and ensured them that the SAM HLG took note of their comments.

AGENDA

Date: *13 February 2017, 13:00-17:00*
Place: *VML/VML SALLE 2, rue Van Maerlant, 2, 1000 - Bruxelles*

13:00 Welcome and introduction to the High Level Group (HLG) and the Scientific Advice Mechanism (SAM)

13:20 Overview of the scientific advice on *Cybersecurity in the European Digital Single Market*, draft findings and observations

13:40 Discussion

14:45 *Coffee break*

15:00 Discussion

16:45 Wrap-up of the meeting

17:00 End

LIST OF PARTICIPANTS AND OTHER ATTENDEES

Participants		
Whalen	Alexander	Digital Europe
Plovie	Anca	Nokia
Nijk	Anjos	European Netork for Cyber Security (ENCS)
Amendola	Antonio	American Chamber of Commerce
Hecht	Brit	BBVA
Hankin	Christopher	Imperial College London
Commers	David	I am the Calvary
Martin	David	The European Consumer Organisation (BEUC)
Broeders	Dennis	Erasmus University Rotterdam; Netherlands Scientific Council for Government Policy
Schulz-Kamm	Eva	NXP
Markatos	Evangelos	European Cyber Security Organisation (ECSO)
Gagliardi	Fabrizio	Association for Computing Machinery (ACM) – Europe
Thomas	Franck	Eurosmart
Van der Linden	Geodele	Marsh & McLennan Companies
Nai Fovino	Igor	Joint Research Centre (JRC) – European Commission
Lozano	Jesús	BBVA
Goodey	Joanna	European Union Agency for Fundamental Rights (FRA)
Korwek	Justine	Trans-Atlantic Business Council
Krahulcova	Lucie	Access Now (member of EDRi)
Meitern	Maarja	Association for Computing Machinery (ACM) - Europe
Realmuto	Mads	UL
Martinez	Martina	Spanish Office for Science and Technology (SOST)
Demerlé	Maxence	Syndicat de l'industrie des technologies de l'information – SFIB
Arpagian	Nicolas	Orange Cyberdefense
Dickman	Peter	Google
Koch	Rainer	Deutsche Telekom
Muir	Stuart	Dell
Caristan	Yves	Euro-Case ; Science Advice for Policy by European Academies (SAPEA) – supported by Horizon2020
Precsenyi	Zoltàn	Symantec
SAM HLG		
Heuer	Rolf-Dieter	
Dykstra	Pearl	
Villani	Cédric	
Bujnicki	Janusz	

SAM Secretariat		
Klumpers	Johannes	
Bray	Jeremy	
Pottaki	Iphigenia	
Gils	Corinne	
Gavigan	James	
Kirk	Stuart	
Martins Branco Correia Lopes	Jennifer	