Briefing for the meeting

with MICROSOFT

25TH MAY 2016, 15.00-16.00
(CAB ROOM)

Topics:

- How technology can help EU countries tackling some of the challenges they face, such as migration/refugee crises or internal and external security threats.
- How to leverage the latest tech developments powered by cloud computing, such as big data analytics or internet of things.

Participants:

- ◆ **From DG HOME:**

-

- ◆ **From MICROSOFT:**

-   at Microsoft

PROPOSED LINE TO TAKE

In the security area, DG HOME aims at pursuing more and more the open source and the full access rights concepts when supporting research and purchase of new technologies by the Member States; this would ensure that the same technology is available to all interested EU public security authorities.

SPEAKING POINTS

- Current migration/refugee crisis and security threats are not the result of any technological deficiencies.

- Nevertheless, technology is important for the EU Member States to face current internal and external security threats.

- The European Agenda on Security adopted in May 2015 acknowledges the role of technology by, for example, including a strong commitment to address the problems of obtaining digital evidence in relation to criminal investigations by 2017.

- The competence for buying security technologies is of the EU Member States.

- It is not in the mandate of the DG HOME or of its agencies, like eu-LISA (EU Large Scale IT Systems Agency), to buy security technologies. The services in DG HOME and in eu-LISA are closely following technological developments in the Justice, Home Affairs and Migration areas.

- Regarding big data analytics and the internet of things, a number of research topics envisaged for the biennium 2014-15 and 2016-17 tackle issues such as digital security (specific call dedicated to it managed by DG CNECT), big data analytics, internet of things, smart borders and digital identity.

- In several of the research topics mentioned above, DG HOME has included specific requirements for the development of open source solutions to be put at the full disposal of the security practitioners.

- DG HOME is currently exploring the possibility of ensuring a follow-up of the security research activities that it is funding within H2020 via other funding instruments such as the Internal Security Fund (ISF).

- One of the envisaged pre-conditions to guarantee such funding could be that the technologies bought by the MS with the ISF is open source.

- Thank Microsoft for their contribution to the EU Internet Forum and congratulate Microsoft for their updated approach to terrorist content online.

BACKGROUND

It is not in the mandate of the DG HOME or of its agencies, like EU-LISA, to buy security technologies. The services in DG HOME and in eu-LISA (EU Large Scale IT Systems Agency) are closely following technological developments in the Justice, Home Affairs and Migration areas.

The competence for buying security technologies is of the EU Member States.

In the area of migration, DG HOME is also not aiming at setting standards/mandatory requirements for the purchase of such technologies by the Member States. So far, what eu-LISA does is a survey of existing technologies.

The European Agenda on Security to fight against terrorism and pave the way towards an effective and genuine Security Union includes a strong commitment to propose solutions by summer 2017, including legislation if required, to address the problems of obtaining digital evidence in relation to criminal investigations. On this basis, the EC has been working closely with NL PRES and will launch an expert process after summer 2016, comprised of several meetings and workshops that will bring together relevant stakeholders, including private companies.

Most recent documents about regular migration are the Communication COM(2016) 205 final "Towards Smarter and Stronger Borders" and the legislative proposal for an EU Regulation (COM(2016) 194 final) "Establishing an Entry/Exit System (EES)".

Current migration/refugee crisis and security threats are not the result of any technological deficiencies. Nevertheless, in the area of migration (regular and irregular), the main current technological needs of the MS concern biometrics (acquisition of images and matching) and the set-up of self-service kiosks. Concerning biometrics, the main challenges regard accuracy and reliability of the used machines and the need is for mobile/portable machines easy to be deployed and used in different contexts (references to the very long terrestrial frontiers in the EU, with not necessarily collaborative neighbouring countries, and to the use of biometric machines on trains)

As future needs in the migration area, we can mention: applications for border crossing done via mobile devices and portable identity documents.

One of the aspects on which eu-LISA will be focussing in the future is also the interoperability of the existing databases managed by them: SIS II, VIS and EURODAC. eu-LISA could also decide to equip itself with a cloud computing system but this should be fully owned by eu-LISA (full European control/ownership of the supporting technology used) and based within the EU.

In terms of research, the H2020 specific objectives for Secure Societies (SC7) cover the development of new technologies and methodologies to help the security practitioners facing the most recent internal and external security threats to the EU. Among others, a number of research topics envisaged for the biennium 2014-15 and 2016-17 tackle issues such as digital security (specific call dedicated to it managed by DG CNECT, big data analytics, internet of things, smart borders and digital identity. The results of these research activities will produce tangible results in 3 to 5 years from the publication of the related research topic. This is the standard duration of the research cycle in this field.

In several of the research topics mentioned above, the EC has included a specific requirements for the development of open source software to be put at the full disposal of the security practitioners. This is needed to ensure that the same technologies developed with EU funds are available to all EU Member States by guaranteeing full access rights to all of them and paving the way to technical interoperability.

The EC is currently exploring the possibility of ensuring a follow-up of the security research activities that it is funding within H2020 via other funding instruments such as the Internal Security Fund (ISF). One of the envisaged pre-conditions to guarantee such funding could be that the technologies bought by the MS with the ISF is open source.

Microsoft is an active member of the EU Internet Forum, which was launched on 3rd December 2015 to tackle terrorist content online. In tackling terrorist content online, DG HOME has two key objectives:

First, to restrict availability of content that promotes terrorism or incites violence online. Here the EU Internet Referral Unit at Europol plays an important role in actively scanning the internet for terrorist propaganda, and then referring it to the companies where it assesses it to have breached their terms and conditions. Through the outreach to the companies, DG HOME has also tasked them to consider a Joint Referrals Platform in order to ensure a more proactive, co-ordinated response and help reduce the 'whack-a-mole-effect'. The DG is expecting results of the industry coalition, and expect Microsoft's active involvement.

The second objective addresses the empowerment of civil society partners to increase the volume of effective counter narratives online. Here DG HOME is developing a Civil Society Empowerment Programme so that it can significantly ramp up the volume of counter/alternative narratives, by providing the technical skills for credible voices to deliver attractive campaigns online.

DG HOME welcomes the announcement of Microsoft's updated approach to terrorist content online, clearly prohibiting terrorist content online, as well as supporting further efforts to leverage new technologies to scan and flag terrorist material: http://blogs.microsoft.com/on-the-issues/2016/05/20/microsofts-approach-terrorist-content-online/#sm.0000kneo6g9eqexiqgi2nbzoamhvb