EUROPEAN COMMISSION
Directorate-General for Communications Networks, Content and Technology

Sustainable and Secure Society
Trust and Security

Workshop report:
H2020: The challenge of providing cybersecurity

Scope & objective:

The Trust and Security Unit at DG CNECT organised a workshop on "Horizon 2020: The Challenge of Providing Cybersecurity" on the 19th of July 2012 in Brussels.

The objective of this workshop was to brainstorm on the challenges, technological gaps and necessary research directions related to cybersecurity and the best suited instruments to implement the tasks. The outcome of this will serve as input to the wider discussion on the thematic orientations of cybersecurity research, development and innovation in H2020.

A group of representatives of the ICT sector was invited. The outcome of the workshop will serve to start the discussion with the stakeholders at large on the content and priorities for cyber security research, development and innovation in H2020 (Horizon 2020).

For the Societal Challenges Pillar of H2020 there will be a particular emphasis on supporting activities which operate close to the end-users and the market. This will include measures to help accelerate the deployment and diffusion of innovative products and services into the market.

Participants:

Markatos Evangelos	FORTH
Bisson Pascal	Thales Sec. Solutions & Services
Barontini Giovanni	Finmeccanica SpA
Bhargava Sandeep	Nokia Siemens Networks
Cuellar Jorge	Siemens
Hogben Giles	Cloud Security Alliance
Cormack Andrew	JANET (UK)
Gomez-Hidalgo Marcos	INTECO
D'Antonio Gianluca	FCC Group
Lotz Volkmar	SAP
Kalbe Gustav	European Commission DG-CNECT
Uriarte Ainhoa	European Commission DG-CNECT
Frederix Florent	European Commission DG-CNECT

Commission européenne/Europese Commissie, 1049 Bruxelles/Brussel, BELGIQUE/BELGIË - Tel. +32 22991111
Office: Avenue de Beaulieu

gustav.kalbe@ec.europa.eu

Results:

a) Background

H2020 will introduce significant changes compared to FP7, in particular in the field of cybersecurity R&D. The Commission proposal foresees to continue in H2020 the industrial roadmap driven research and development under the "Leadership in Enabling Indsutrial Technologies " (LEIT) Pillar. This is the direct extension of the "Trustworthy ICT" R&D Program of FP7. The novelty in H2020 will be the extension of research and development activities to innovation activities in the "Secure Societies" (SC7) component of H2020 Societal Challenges Pillar.

The objective in SC7 is aligned with the general aim of the Societal Challenges Pillar, i.e. to support more innovation and have more research results translated into products. In SC7 this is extended by the consideration that the ICT we use could be more secure if we were more systematically deploying existing state-of-the-art security solutions. But in the absence of a clear user demand and missing incentives for the suppliers there is neither a market, nor wide spread adoption of secure ICT.

This is what SC7 intends to change: increase the availability and uptake of secure ICT. The intention is to use the H2020 Program to support and trigger this change of market landscape and reduce the financial risk of the stakeholders.

The SC7 is not only an extension of the Trustworthy ICT activities of FP7 into addressing the societal challenge of cyber security, but will also be a vehicle to implement the actions defined in the upcoming European Strategy for Cybersecurity.

b) Outcome of the discussion on the content

The brainstorming identified a number of **challenges** that need to be addressed to increase the overall level of cybersecurity. They can be broadly regrouped into five areas that need attention:

1. *Addressing the needs and perspective of the user (in its widest sense, i.e. individuals as well as corporate and public administrations):*
   - **Usability** and effectiveness of secure ICT products and applications, or security features according to a risk based approach;
   - The public **perception** of cybersecurity;
   - **Education** and understanding of ICT security issues;
   - **Awareness** that the usage of ICT has some risks and that the user has to protect himself and others;
   - Most current security **policies** are not user centric.
2. *Building capabilities:*
   - **Deterrence** – cybersecurity is asymmetric, i.e. the effort spent for protection is by far higher than the effort needed to perpetrate an attack;
   - **Intelligence**: – there is no central trusted source of information of what is going on.
   - There is not sufficient **secure data sharing** on vulnerabilities, incidents and risks.
   - Insufficient **Public-Private** partnership in ensuring cybersecurity.
3. *Making cybersecurity a positive business case:*
   - **Economics** – there is no reliable data on the real cost of cybersecurity;
   - Proposed security solutions, or the additional cost for security features do not appear **affordable**;

- Feedback on the **quality** of the security level of a product, or the quality of security is missing.

4. *The role of technology:*
   - **Security by design** – Security features are an add-on, or are proposed as patches. They are not a driving specification in the design of ICT;
   - **Poor SW development** – SW is released on the market prematurely in order to secure the market;
   - There is no **risk management** culture;
   - What are the **security enablers**?
   - Security solutions are 'all or nothing', they are not **scalable** in function of the potential risk or complexity of the underlying system;
   - **Technology agnostic** – Current security solutions are specific to the device or application they are running on.
5. *Defining cybersecurity metrics:*
   - The current **timing** of funding measures implemented by the European Commission does not allow to react quickly to an emergency;
   - **Compliance** – At EU level there are no commonly agreed rules, norms or best practices with respect to security;
   - **Benchmarking** – Competing products are difficult to compare on the performance of their security features;
   - There are no reliable **statistics** on the number, size, impact, origin, etc… of attacks;
   - Many of the popular applications (e.g. social networks) or devices are **not developed in Europe**;
   - Security **certification** (of products and people) is time consuming and not mandatory for many daily applications or devices.

c) Outcome on the discussion on funding instruments

In order to address the challenges for cybersecurity what would be the best suited **funding instruments**? Without associating a particular instrument to a particular challenge, the following instruments were proposed:

1. **R&D activities**: experimental research, maturing R&D projects;
2. **Demonstrators**: large scale pilots, large scale demonstrators, feasibility demonstrators, proof of concept projects, deployment projects;
3. **Infrastructures**: public innovation labs, prototype manufacturing lines, technology survey observatories, simulation laboratories, cloud infrastructures as a service, cyber exercises, EU certification authority, verification of system health and consequent 'vaccination', seed funding for helpdesks (e.g. botfrei), security hotlines;
4. **User support**: training and education of individual and corporate users, EU security university, awareness programs, community building;
5. **Incentives**: call for tenders, early adopters support, pre-competitive public procurement, support for business to pick up security solutions, business plan competition, industry programs, co-investment, reduction of red tape, security awards.

Next steps:

The outcome of this workshop will serve as input to start the discussion on the orientations of cybersecurity activities in the Societal Challenge 'Secure Societies' in H2020.