NIS Platform

Minutes of the first Meeting of

WG3 on Secure ICT Research and Innovation

September 27, 2013; 10h00-17h00

European Commission

Brussels

1. Introduction

The Commission opened the meeting and explained that WG3 will become its main stakeholder platform to devise the European secure ICT Research and Innovation agenda, with a key focus on turning research results into products.

The Chairs of WG3 offered a quick clarification of the purpose of the meeting, as follows.

   a. Get participants to know each other;
   b. Share the Terms of Reference draft and ask for contributions with deadline October 4th;
   c. Share knowledge and establish connections around content towards the Strategic Research Agenda (SRA) to be produced by the group;
   d. Make emerge a structure that facilitates the execution of the work;

The Commission described the general organisation of the NIS Platform and the specific mandate of WG3. It clarified that the NIS Platform is an inclusive and multi-stakeholder platform, driven by the participants. The work within each group will be steered by the WG chairs, with the help of a secretariat provided by the Commission and ENISA. The progress of each group will be discussed at the next plenary meeting of the NIS Platform, scheduled before the end of the year.

A *Tour de Table* was organised, with a special focus on the opportunities participants see in WG3. The main opportunities identified include: gaining knowledge, securing funds for and ensuring collaborative research, shaping and influencing the SRA, ensuring that efforts are made towards standardisation, and addressing societal challenges for public benefit (e.g. e-Health, e-Democracy, social technologies, cybercrime, cyber strategy, cybersecurity, infrastructures, children's e-security, green security, and transportation).

The Chairs presented WG3's draft Terms of Reference and asked for contributions to be shared in the online platform by October 4th at the latest. The Terms of Reference should be finalised by mid-October.

The Chairs presented the deliverables that are expected from WG3 – Secure ICT landscape plot; Business cases and innovation paths; Snapshot of education and training offer; and Strategic Research Agenda (SRA) – and asked for expressions of interest for taking leadership of a deliverable. Motivated expressions for interest should be submitted by email to the Chairs by October 4th.

2. Questions and Answers

The chairs and the Commission took questions from the floor.

The Commission clarified that the scope of work should be defined by the group. In particular, it should not necessarily be limited to critical infrastructures. The Commission clarified that the work of the group will feed into the EU research work programmes from 2016 and beyond, as the Work Programmes 2014/15 are already drafted. Finally, the Commission clarified that all topics addressed by WG3 could potentially be included in H2020, since cybersecurity is a cross-cutting issue that pervades all ICT-related topics. Against this background, it will be important to make sure that all relevant stakeholders are involved in the work of the group.

As regards the link between WG3 and national research programmes, the chairs explained that the WG3 will involve national roadmaps and national representatives' feedback. In general, the coordination between the three working groups of the NIS-Platform will be ensured by the working group chairs but also by individual participants who take part in more than one working group. In order to achieve a successful finalisation of the SRA in 2015, participants are invited to contribute actively in the meanwhile by preparing intermediate deliverables and implementing guidance, e.g. on business cases and innovation paths.

3. Areas of work

Because of the paradigm shift envisaged in Horizon 2020, where Societal Challenges are at the centre of the call for proposals in the area of Secure ICT, the participants were requested to generate visions of aspirational futures in 2025 in order to inform the works towards the design of the SRA. The many inspirational visions that emerged were clustered by the participants into five main areas of interest, that were provisionally entitled as follows.

1. Citizen and people-centric computing
2. Interconnected society
3. Privacy, security and civilisation
4. Resilient infrastructures and services
5. Multi-disciplinary skills, knowledge and awareness

After lunch, the groups were asked to define, in break-out sessions, the content and management of each of these areas. The issues to be addressed were the following.

a. What are the challenges related to Secure ICT in this area?
b. Gap analysis from what exists today to what needs to be developed
c. Milestones towards the Delivery of the SRAs
d. Working Methods & Organisation
e. Action Points
f. Next steps

Each group appointed a host and a rapporteur and carried conversations around its topic. The hosts and rapporteurs briefly reported back in plenary about the issues addressed, in particular on the content of each group, but also, whenever possible on its next activities:

1. <u>Citizen and people-centric computing</u>

Challenges included: to provide much more technology in the future but ensuring freedom, security, fairness, usability, understanding of consequences and risks, existing gaps between technological and legal, policy and technology, implementation of capabilities, and governance.

Needs included: workshops not only discussions, diversity of stakeholders, networking, and a decentralised approach.

2. Interconnected society

Challenges included: an EU ecosystem different from a global ecosystem and a natural secure usage of technology based on social values.

Needs included: business cases for education and for technologies like Facebook; definition of what is natural secure usage of technology; expert input on how to address this and keep a lifelong education on this.

3. Privacy, security and civilisation

Challenges included: secure and privacy by design in mobile devices, lack of user control, data and processing, ethics and product development, ID fraud, lack of usability, risk awareness and management, freedom of speech and censorship, and cost effectiveness.

Needs included: standards, governance, better practice of credentials, and frameworks.

4. Resilient infrastructures and services

Challenges included: awareness of security needs, measurable security, security and interoperability in complex environments, including security of the supply chain, security of legacy systems, joint consideration of safety & security, manageable cost and performance of security.

Next steps included: mapping of state of play, business cases, including based on certification, and innovative cases (pilot projects close to market).

5. Multi-disciplinary skills, knowledge and awareness

Challenges included: awareness of consequences of improper use of technologies, privacy which matches technology advances, multidisciplinary skill-set at all levels, and easy access to knowledge.

Next steps included: engage experts, methodologies for research to see what education and curricula should contain/ cover; create components for CV, aggregate knowledge portal and repository modules to be used in education.

It was agreed that the groups' conversations would continue remotely, ideally on the online portal provided by ENISA. Each host will provide a written summary of the topics discussed by the groups by October 4th.

4. Conclusion

The Chairs thanked all participants for having attended the meeting and for having collectively and actively worked towards the initial definition of the SRA's topics. They underlined that the work is only starting and urged participants to provide the first inputs as agreed.