

Newsletter

WG3 Secure ICT: Research and Innovation

of the NIS Platform

This second edition of the WG3's newsletter covers the WG3 Meeting that was held on July 16, 2014 at the European Commission, in Brussels (BE). This meeting provided opportunities to synchronize with different EU related initiatives and funded projects as well as to check the state of play of WG3 deliverables by discussing priorities, findings and opportunities, specially related to the SRA (Strategic Research Agenda) deliverable.

The structure of WG3 is designed to facilitate cooperation among its members in order to add value as active contributors, so there were interactive sessions, as usual.

The Working Group 3 of the NIS Platform addresses issues related to research and innovation in Secure ICT.

The NIS Platform is an inclusive and multi-stakeholder platform driven by the participants and consists of 3 working groups. It is part of the European Strategy for Cybersecurity (see [IP/13/94](#)). The NIS Platform serves the two priorities of this strategy: achieving cyber-resilience and developing industrial and technological resources for cyber-security.

The NIS Platform will provide the groundwork for the implementation of the proposed NIS Directive (see [MEMO/13/71](#)).

Guidance from the NIS Platform will feed into Commission recommendations on cyber-security to be adopted in 2014.

<https://resilience.enisa.europa.eu/nis-platform>

E-mail contact: CNECT-NIS@ec.europa.eu

On July 16, 2014, more than 50 participants attended the fourth physical meeting of the Working Group 3 of the Network and Information Security Platform on Secure ICT: Research and Innovation. Jakub Boratynski, Head of the Trust & Security Unit at DG CONNECT, opened the meeting and confirmed that the first results coming from the group in the form of the report on Secure ICT Research Landscape was very well received by the European Commission and stakeholders. He also confirmed that this group is seen by EC as one of its main advisory body to devise the Strategic European cyber security Research and Innovation agenda, contributing to H2020 programme strategy.

Objectives

The Chairs of WG3, namely Fabio Martinelli, Security Group Instituto di Informatica e Telematica, CNR, IT, and Raúl Riesco Granadino, Head of Research & Development (R&D), INTECO, ES, clarified the meeting objectives:

- Synchronization and cross fertilization among EU projects and WG3 (keynote speakers invited);
- Check point for the assessment of the deliverable status;
- Promote and organize further Work on the next activities per deliverable (specially, the cross-analysis phase for all Aol's inside SRA).

They also described how the SRA deliverable (in progress) will embed the different deliverables (*Research Landscape, Business cases & innovation paths and Education & training for workforce development*).



Figure 1: As a recap, this was the word cloud of participant's expectations at the kickoff meeting of WG3 in September 2013

Synchronization among EU projects

The meeting was designed, as usual, in a highly participatory manner. As a starter, we launched a synchronization and cross fertilization round session by inviting keynote speakers from EU related projects and initiatives mainly focused on security research road-mapping.

In this session, and during the first part of it, participants had the opportunity to listen to different keynotes from European Parliament, European Defence Agency, Dutch Member State, as well as EU funded projects like IPACSO, CAPITAL and CAMINO.

There is a great opportunity to share knowledge, experience and visions from other domains and several related initiatives towards cybersecurity research foresight

As a result of this first part, participants:

- Had the opportunity to know and participate in the policy related *European Parliament (LIBE)* call for paper (CFP) opened until Oct 31st,
- Shared knowledge and experience on road-mapping with other sector/dimension (*Defence sector*),
- Had the opportunity to learn about the Dutch National SRA,
- Synchronized with EU funded projects like IPACSO, CAPITAL and CAMINO.

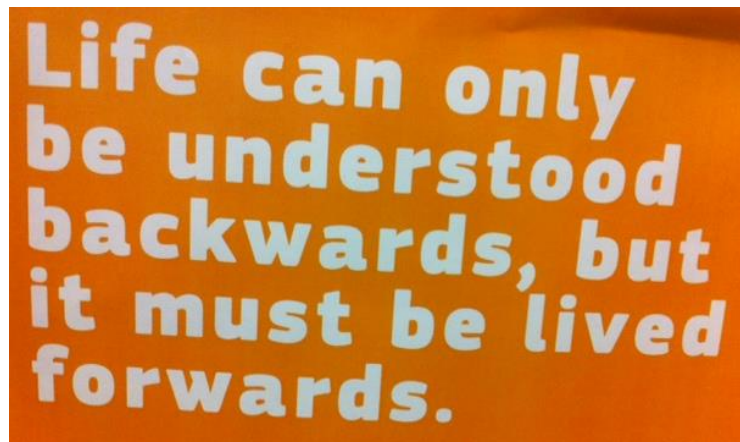


Figure 2: Creative quote in the room (by Soren Kierkegaard)

WG3 deliverables' state of play

During the second part of the meeting, participants had the opportunity to check the state of play of the different deliverables of NIS WG3 committed by its ToR (Terms of Reference).

All WG3 members have access to the last version of each deliverable state of play through ENISA portal (<https://resilience.enisa.europa.eu>).

As a first major milestone, the “Secure ICT Research Landscape” deliverable first release, was presented by its editorial team.

They described the process followed as well as the major findings. As the first WG3 deliverable released, it represents the security research state of play at European level, as well as it identifies the first technical research gaps. Those will be treated as inputs by the SRA deliverable.

The Secure ICT Research Landscape deliverable is useful to have a clear picture of EU security research state of play, challenges, gaps and existing tools under a technology perspective.



Figure 3: Interactive small group of discussion

Regarding, the “Business cases and innovation paths” deliverable, the editorial team made a presentation of different interesting aspects for the creation of the document as well as the state of play.

They described the methodology being used, the market overview, the persistent trends (especially those which could drive the EU economy growth), and the identification of use cases, innovation models and incentives. Those will also be treated as inputs by the SRA deliverable inside the prioritization and x-analysis phase.

The “Business cases & innovation paths” deliverable will examine ways to increase the impact and commercial uptake of research results in the area of secure ICT including via innovative financial instruments and funding methods as well as new business models.

As a result, NIS Directive and EU Cyberstrategy are kept in mind in this deliverable as it should be an input for the European Industrial Strategy.

We are interested on how new business models and innovations paths may form a kernel for a new generation of European industry which will foster economic growth in Europe

Regarding the “Education and training for workforce development” deliverable, the editorial team made a presentation of the state of play, especially the data collection phase by presenting their first coordinated results together with ENISA NIS Driver license group¹.

They described the methodology being used as well as first findings. There is a need to collect more information from other dimensions like electrical engineering, law, political science as well as some other EU countries data still missing today.

First findings were announced like the lack of interdisciplinary education, the lack of a widespread mechanism for sharing knowledge and materials, and the lack of a comprehensive scientific foundation in

¹ ENISA is working on the Roadmap for NIS educational programmes in Europe so a common goal has been identified with NIS WG3.

the area of Cybersecurity. The results of this deliverable will serve as input to the SRA and are meant to be evolving, since new SRA topics will identify the need for developing new skills.

The “Education and training for workforce development” deliverable will produce an analysis of available offers in higher education and training in cybersecurity in Europe and beyond.

Notably, during the meeting, a quarter of the attendees confirmed that they had multidisciplinary background (law, economics, politics, geography, philosophy, history and insurance) in addition to cybersecurity.

The case of SRA (Strategic Research Agenda) and AoI (Areas of Interest)

Once Chairs explained that SRA embeds the rest of deliverables, a presentation of each layer (Area of Interest: individual, collective/supply side and infrastructures) took place by the corresponding leaders. Those are:

- Area of Interest 1: Individuals' Digital Rights and Capabilities (Individual layer)
- Area of Interest 2: Resilient Digital Civilisation (collective layer)
- Area of Interest 3: Trustworthy (Hyperconnected) Infrastructures (Infrastructure layer)



Figure 4: As a recap, this was the word cloud of priority areas that emerged at the kickoff meeting in September 2013

Aol # 1 – Individual layer represents the user centric view, that is:

...how to design, manage, and control network and information and communications technologies respecting privacy, fairness, democracy, freedom of expression, safety enhancing technical aspects by social, legal and regulatory aspects of security and privacy.

It includes

- respect for citizens and consumers.
- transparency (without intrusiveness) to be provided at all times.

Aol#1 leaders presented their first findings about enablers and inhibitors, such as technological, economical, societal, and regulatory.

Aol # 2 – Collective layer represents the supply side...

...ensuring that digital institutions of society are as trusted in their digital forms as they are in physical form; in a way this is the 'supply side'.

Organisations operate under a whole series of obligations – regulation, contracts, societal norms, and must manage risks, ensure security, and handle information securely and respecting fundamental rights of the customers/citizens.

Aol # 2 leaders presented their methodology followed. In summary, new technology adoption in 2025 will imply a change in the threat landscape which will create new emerging risks and new security impacts.

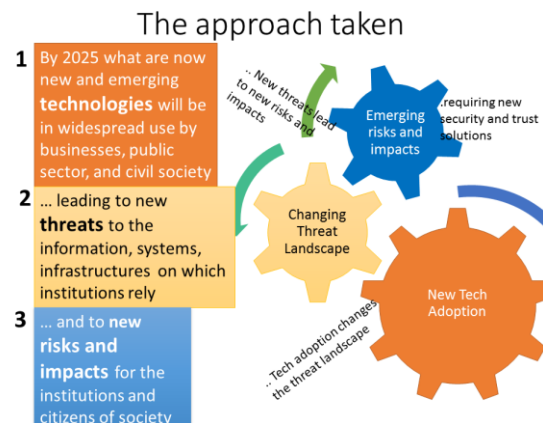


Figure 5: approach taken for AOL2 2025 visions discussion

The survey conducted inside the subgroup included the following questions:

- What are the new threats for 2025 arising from new technology adoption for each of the topic?
- What are the risks and impacts of those threats?
- What are the gaps and barriers and potential solutions to address them all?

The outcome resulted in a list of identified research gaps that were presented during the meeting. They include new forms of protection from fraud stemming from digital currencies, end to end secure data channels, security, and dependability.

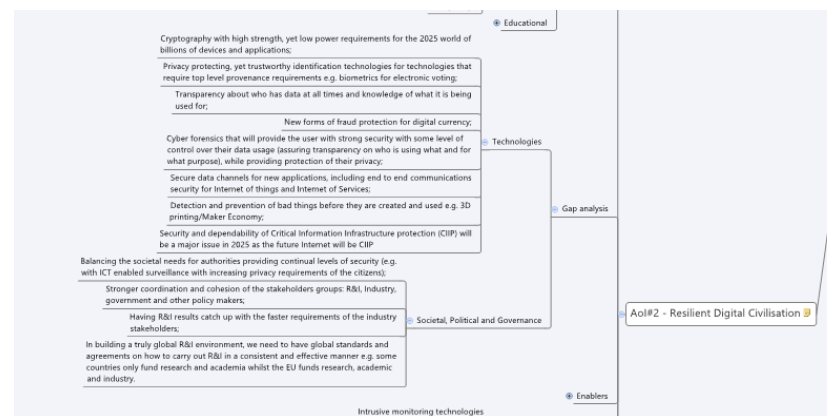


Figure 6: Mind map of AOL#2 gap analysis

Aol # 3 – third layer represents the Trustworthy (Hyperconnected) Infrastructures ...

...ensuring security and continuity of infrastructures and systems – so that the economy and institutions can operate.

Infrastructures and systems need to be secured against threats and failures to ensure the continuity of the institutions and services they support.

Aol# 3 leaders presented the state of the art today and asked for more contributors in specific sectors, like automotive, energy, smartgrids, and finance.

The document uploaded at ENISA platform (work in progress), is very detailed and has a good level of description.

The subgroup provided a first list of prioritized and dependent sectors as well as enablers and inhibitors.

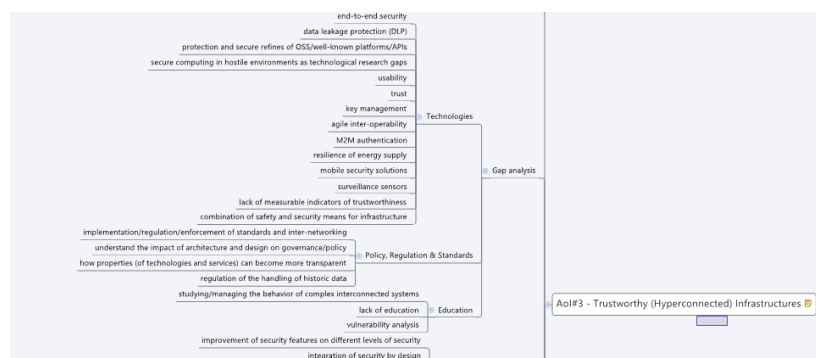


Figure 7: Mind map of Aol#3 gap analysis

The interactive session: Cross-analysis phase

The Cross-analysis subgroup leaders presented their first findings (note that the work is still in progress by each of the Aols). After the presentation, all the participants were asked to answer in different groups the following questions:

- Panel 1: "Are inhibitors mostly of non-technical nature? Are there others?"

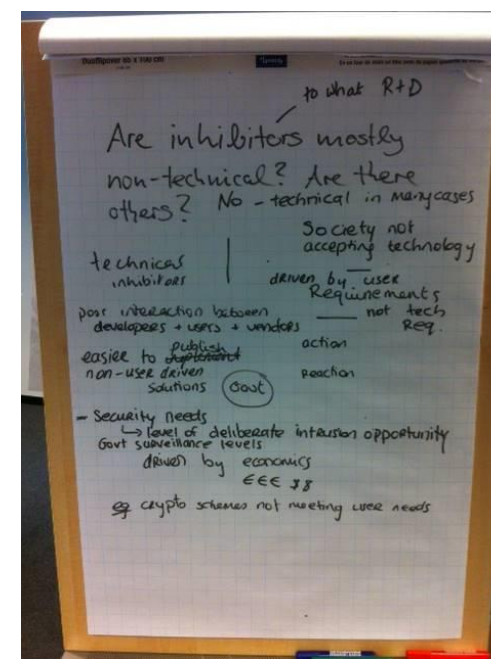


Figure 8: Screenshot of panel 1

- Panel 2: “Which contributions have the potential to disrupt the market?”

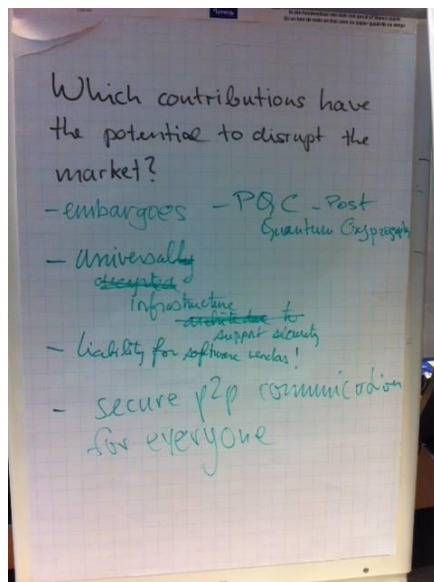


Figure 9: Screenshot of panel 2

- Panel 3: “Do we need evolution or disruption?”

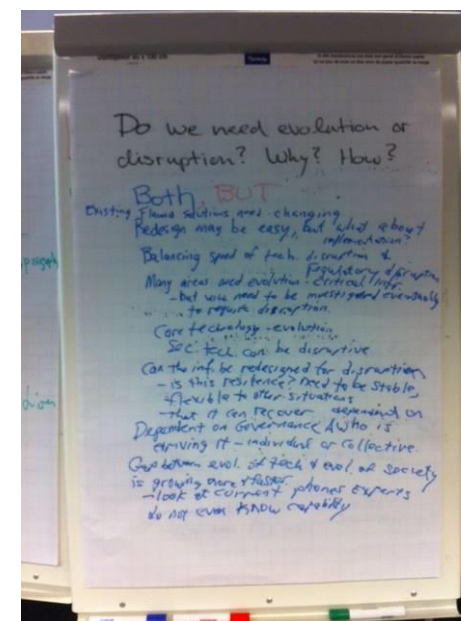


Figure 10: Screenshot of panel 3

- Panel 4: “How was the threat landscape evolving?” - Who/Why (motivation)/ How + accidental
- Panel 5: “Who should be responsible for cybersecurity?”
- Panel 6: “What should happen in the area of secure ICT over the next 5 years?”
- Panel 7: “What should be avoided?”



Figure 11: A group of interactive discussions for the x-analysis phase

Each group appointed a *leader* and carried deep and meaningful conversations around its topic. At the end of the time allocated for such conversations each of the panel leaders gave a brief explanation of each of the panel discussions and agreements to all WG3.



Figure 12: Briefing of Panel 6 to all WG3

The answers are really helpful for X-analysis leaders to start their prioritization phase by providing some important clues as inputs.

Again, a great and participatory meeting! - Sharing expertise and experiences:

Some statements made by participants about the day:

"Defence sector has similarities with cybersecurity like ICS or APT but 20% non detection is not acceptable"

"I was surprised by the openness of conversations, exemplified by the Defence sector intervention -- Unclassified information can easily be shared --"

*"This was a very motivating meeting. Thank you for inviting us.
(keynote speakers)"*

"Again we took the risk of innovating in the meeting facilitation process. It was worth taking!"

"WG3 is really a great multidisciplinary team. More than 25% of WG3 attendees today have another non-technical background: Law, Economics, Politics, Geography, Philosophy, History, Insurance, etc."

"The WG3 has been invited to share its findings and recommendations with the H2020 Strategic Advisory Group (SAG) (10 Sept) and the H2020 Programme Committee (30 Sept)"

"We all agree that Cybersecurity must be everyone's responsibility"

Further steps

1. Next meetings

Next NIS WG3 meeting takes place on 8 October, 2014, in Florence, the day before the ICT Proposers Days and aligned with EC-funded projects CAPITAL and CSP Forum.

2. Further debate

The WG3 Chairs continue to have separate conference calls with deliverables' editors and Areas of Interest's leaders to provide a comprehensive approach to the Cross-analysis prioritization phase.

The Chairs, the editors, and the leaders compose WG3's Steering Committee. Its current composition is the following:

Fabio Martinelli (WG3 chair / SRA deliverable editor, CNR)
Raúl Riesco (WG3 co-chair / SRA deliverable editor, INTECO)
Pascal Bisson (SRA deliverable editor, THALES)
Paul Kearney (Business cases & innovation paths editor, BT)
Paul Malone (Business cases & innovation paths editor, TSSG)
Zeta Dooly (Business cases & innovation paths editor, TSSG)
Bart Preenel (Secure ICT Landscape editor, LSEC)
Evangelos Markatos (Secure ICT Landscape editor, Forth)
Javier López (Secure ICT Landscape editor, UMA)
Mari Kert (Secure ICT Landscape editor, EOS)

Claire Vishik (Education & training editor, INTEL)
Maritta Heissel (Education & training editor, Duisburg Essen)
Kai Rannenberg (Aol#1, MChair)
Gisela Meister (Aol#1, G&D)
Nick Wainwright (Aol#2, HP Labs)
Jim Clarke (Aol#2, Waterford IT)
Steffen Wendzel (Aol#3, Fraunhofer FKIE)
Piero Corte (Aol#3, Engineering)
Neeraj Suri (X-analysis leader, TU Darmstadt)
Volkmar Lotz (X-analysis leader, SAP)

Afonso Ferreira (WG3 Secretariat, European Commission)