CONCLUSIONS AND NEXT STEPS

A final dedicated session on the future planning and operations was designed to set out where the BIC project and the community will go in the next period, and to discuss what the trust and security research community would need in terms of support for these activities.

The chairs from the technical sessions started the session with a short summary of the recommendations made within their panel sessions.

Session 1: Opening session and panel of INCO projects.

James Clarke presented the recommendations from session 1:

- **Implement technical platforms or longer term initiatives apart from projects alone** (something lasting and that can help cooperation between multi-countries
- **BIC should talk to SECAS** partners about their **experiences** (see if their methodologies and approaches would be of use to BIC)
- **BIC** may help to develop **content** for upcoming **BILAT** workshops.
- **Efforts should be made to dramatically increase** visibility of RTD programmes.
- In addition to Working groups, look at possibility of setting up permanent **Action Groups** to improve collaborations (currently recommendations are highlighted but nothing is implemented, which leads to frustration amongst the key stakeholders)
- It is good to **take stock** of current INCO projects, to provide greater clarity on what important topics we want to focus on.
- **Bi-lateral** approach and initiatives are still very important and necessary, even when trying to establish a parallel **truly global community**.
- **Collaborations** between various countries will be at **different levels**, and over time could improve taking **ideas or building on experiences** from other countries established collaborations. **Patience is required**.
- **There is a need to co-ordinate** activities of INCO across **all areas (as an umbrella)**, to get a bigger picture of what's going on.

Session 2: Human Oriented Approaches to Security.

Priscila Solis Barretto presented the recommendations from session 2:

- It is important to consider that we are in a globally connected world with **different generations** of users.
- We need **the adaptation of experts** to what users need, not the contrary (**user centricity**).
- **Multidisciplinary workshops and building international working groups** is necessary, e.g. multi-disciplinary experts on human oriented security.
- Build **local expertise** and then establish key **international linkages**: local expertise based on local demands and then participate together in coordinated calls for formal cooperation.

- Development of solutions that take into account the **different social structures** (BRICs, developing countries, etc.).
- **Availability of Funding mechanisms:** good will is important but there must be a political work between agencies in the different countries to be successful.
- **Cooperation activities** to compare tools and techniques, avoid duplication, validation of case studies and shared testbeds **in different environments** and **cultures**.

Session 3: Digital ecosystem and network information security.

John C. Mallery presented the recommendations from session 3:

- As a community, we should pick the highest priority topics in network security and develop an **overall international R&D plan for policy makers.**
- Focus on **mutually beneficial topics** for **international cooperation:**
  - International data exchange architecture for cybersecurity;
  - Open source trustworthy host platform for collaborative research and education;
  - Cryptology;
  - Mobile Security of Software Services;
  - Joint exercises related to cybersecurity
- **Identify** R&D expertise in the relevant fields.
- Form a **planning group to get maximum impact.**
- Cryptography - Like to have **world scale competition**
- **Ecrypt II roadmap for next 10 years –** crypto for cloud computing/Internet of Things
- In the US, NIST drives crypto policies, in Asia, crypto policy is by country, **Europe joint research policy by country.**
- **We Need to bridge gap between research interaction with policy/**
- Algorithms – **More open competitions** with shared governance
- In order to foster Joint research – we need to **go beyond meetings.**
- Mobile applications – e.g. mobile health care, data storage – **threats lead to wider implications.**
- **Focus on** policy framework, build prototypes for DDOS, secure new services, mobile security.
- **Lessons** taken from the **EU – US Cyber exercise** should be taken on board and more of these kinds of exercises should be organised.
- In Japan, there is a large scale **International Project on Cybersecurity**. It should be checked as to the feasibility of forming co-operations around this.

BIC Working / Action Groups

Michel Riguidel presented a summary of the work items in which working groups would be established and supported by BIC. It would be the intention of the project to additionally form longer term action groups based on the successful outcomes of these working groups.

WG1. Human oriented /citizen security focus, which as a starting point would focus on the following topics:

- End to end trust assurance for users;
- Usability / user interface designs;
- Addressing prediction, validation and enforcement mechanisms needs and requirements;
- Putting users in control of their data and information;
- Taking into account cultural aspects.

WG2. Network Information security / Cybersecurity, which would focus on:

- International data exchange architecture for cybersecurity;
- Open source trustworthy host platform for collaborative research and education;
- Cryptology;
- Mobile Security of Software Services;
- Joint exercises related to cybersecurity.

WG3. Programme /funding focus/ identify community, which would focus on:

  - Identifying stakeholders (contacts in programme management and research communities);
  - R&D Planning/R&D experts of excellence;
  - Raising programme visibility.

If interested to participate to these working groups, please contact **michel.riguidel@telecom-paristech.fr** and **jclarke@tssg.org**

Finally, in order to increase the networking potential of the international trust and security community, an international research network portal is being set up by the BIC project to enable a one stop shop for trust and security researchers from all countries. The information will be accessible and searchable by country, research topics, projects, and other criteria. The portal will also provide access to researchers other well established sites – LinkedIn, personal web sites, blogs, ..A number of people from the International research community have already volunteered to participate in the BIC portal in the first draft. Additional volunteers are welcomed to **jclarke@tssg.org.** An example screen shot is shown in Figure 1:

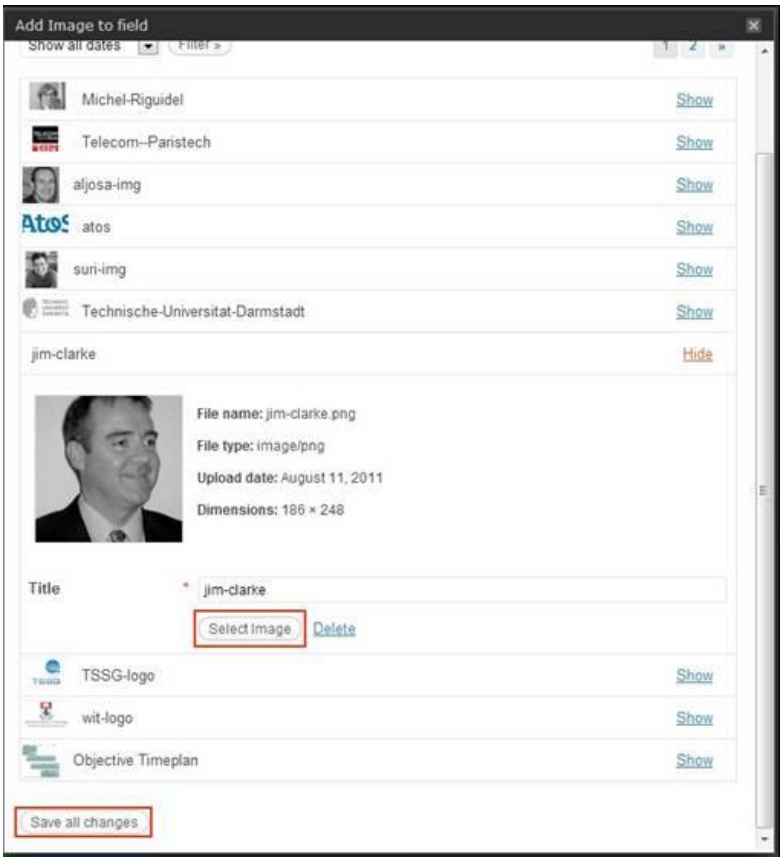

Figure 1. BIC Research network portal – data entry page

Acknowledgments

The BIC project is funded under Call 5 of FP7 ICT and began on 1st January 2011 with a duration of three years. The project is supported by the European Commission DG INFSO, Unit F5 ICT Trust and Security Research[1].

[1] http://cordis.europa.eu/fp7/ict/security/