D4.6 BIC Annual Forum and IAG meeting 2012

Grant Agreement number: 25258655

Project acronym: ***BIC***

Project title: Building International Cooperation for Trustworthy ICT: Security, Privacy and Trust in Global Networks & Services.

Funding Scheme: ICT-2009.1.4 [Trustworthy ICT]

Project co-ordinator name, title and organisation:

James Clarke, Programme Manager, Waterford Institute of Technology

Tel: +353 71 9166628

Fax: + 353 51 341100

E-mail: jclarke@tssg.org

Project website address: http://www.bic-trust.eu

Table of Contents

Executive Summary

To raise the impact for both International cooperation (INCO) projects' annual forum events, the FP7 projects BIC [1] and EuroAfrica-ICT [2] held their events together over the dates 27th – 29th November 2012 in Lisbon, Portugal.

On the 27th November 2102, the BIC project held their International Advisory Group (IAG) workshop during the morning and an open workshop on international cooperation covering trust management for mobile services during the afternoon. Further information on the event can be found at http://www.bic-trust.eu/events/.

On 28-29th November 2012, the EuroAfrica-ICT held their 2012 Africa-EU Cooperation Forum on ICT Research. Further information on the EuroAfricaICT Annual forum can be found at [1]. The BIC project, including members of the BIC IAG, were involved in the organisation and participation of a specific session held on 29th November 2012 entitled ***Session 3D: Cyber Security & Trustworthy ICT.*** The results of that session are reported separately in [18].

The following report documents the BIC IAG Annual Forum 2012 event [3] held on 27th November 2012 in order to capture the main discussion points and agreements on the way forward.

The main conclusion of the workshop was that increased effort is needed to address the threats in cyberspace – the networks themselves, their legitimate users, and their systems and services. The following key areas were identified:

- countermeasures for cyber crime, and cyber forensics;
- identity management frameworks for people, multimedia content, the *IoT;*
- the widening scope of threats towards applications and direct expressions, with disinformation, defamation, denigration, e-revolt;
- the extensive and fragmented spectrum of attack organizations.

For all these issues, only a global approach can be effective; this must involve all the major actors: commerce and industry – equipment and services; research organisations; administrations – legal and regulatory frameworks. Priority should be given to the following:

- Mobile Security;
- Mobile Cloud Computing Paradigm = mobile + cloud security;
- International data exchange architecture for cyber security;
- Identity, Privacy;
- Trust management models;
- Security as a Service.

In the second year of BIC during 2012, the project has taken a lead role in developing and promoting a longer term strategy that is based on the need for the expansion of the current mechanisms to include both bi-lateral (tactical) and multi-lateral (strategic) elements, which seems to match the direction being taken by the Commission for their 'strategic thinking' on INCO for Horizon 2020 [19]. However, as these new proposed longer term structures are beyond the original scope of the BIC IAG and WGs, focus in the next year should include finding mechanism(s) for continuing and advancing this BIC initiated work into H2020 after BIC concludes.

If you have any questions on any of the material in this report, please make contact with the BIC coordinator, Jim Clarke jclarke@tssg.org.

1. Introduction

The purpose of the European Commission funded BIC coordination action project (http://www.bic-trust.eu/ is to foster cooperation between the EU and the international programme agencies and researchers in India, Brazil and South Africa within the focus areas of Trustworthy ICT, including trust, privacy and security, in order to:

(a) Understand the activities and planning of the target countries; and

(b) Carry out a mapping of the European Commission's planning to them, such that a common technical and policy alignment is viable.

The building of international cooperation (INCO) is a collaborative effort that only works if it reflects the views and priorities of the target countries as well as buy-in from technical experts of the EU along with the target countries.

The majority of the current approaches towards INCO have been based on a bi-lateral basis (country to country - tactical level) as shown in figure 1.

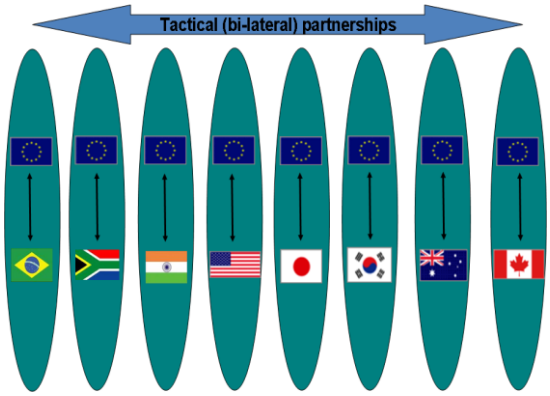

Figure 1. Tactical (bi-lateral) approach

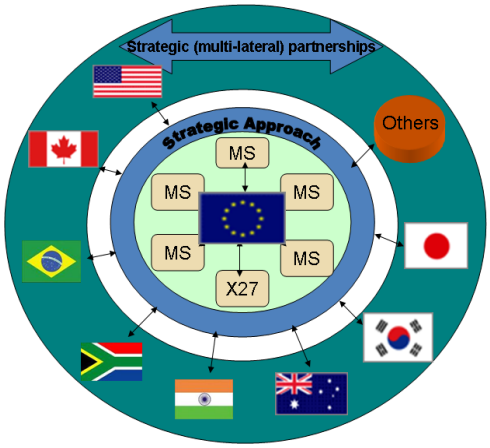

Figure 2. Strategic (multi-lateral) approach

While this approach may work for higher level themes, difficulties arises when a research topic such as cyber security needs to be addressed globally and multi-laterally amongst many regions. Therefore, the BIC project is examining the feasibility of a more strategic approach based on multi-lateral partnerships as shown in figure 2, in addition to the International Advisory Group (IAG) supported by Core Working Groups (CWG) as shown in Figure 3.

The areas and scope of the three working groups are the following:

1. **WG1. Human oriented /citizen trust, privacy and security**, which will focus on topics related to a multi-disciplinary approach for international cooperation amongst all stakeholders;
2. **WG2. Network Information security / Cyber security**, which will focus on topics related to the need for international cooperation for enabling the protection of networks and systems;
3. **WG3. Programme /funding focus/ identify community**, which will focus on the requirements, processes, mechanisms and barriers to enable collaboration opportunities.

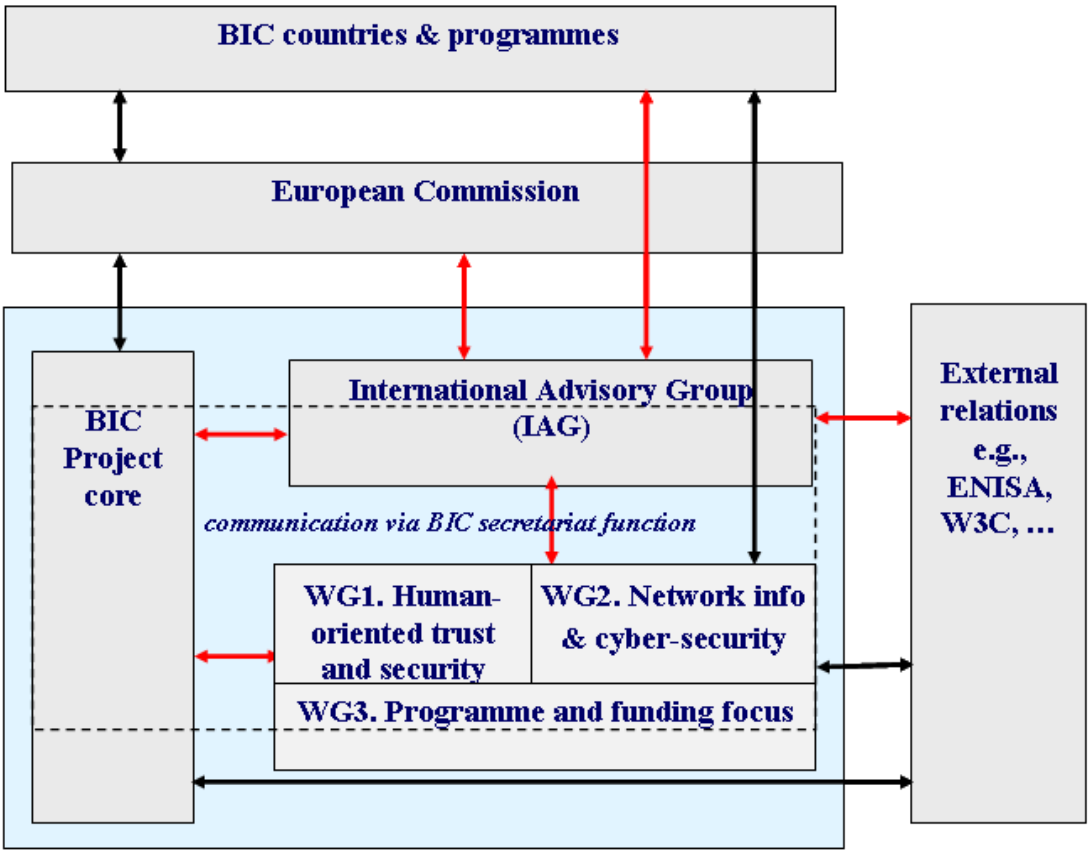

Figure 3. Overall structure of BIC project and external bodies

International Advisory Group (IAG)

The BIC IAG committee is composed of members from the BIC partner countries, together with representatives from countries involved in earlier INCO work. It is tasked with identifying a roadmap for collaboration activities identifying:

- Prioritized areas of collaboration of technical themes (short & long term),
- Types of cooperation activities (projects, repositories, test beds, exchanges…),
- Timelines and road mapping,
- Support mechanisms and potential for alignment of cooperation calls,
- Forum(s) for exchange,
- Success parameters and metrics for cooperation effectiveness.

The IAG has representation from the participant countries from both the researcher communities and programme management (funding agencies). The IAG's role is to suggest and formulate the policies, processes and mechanisms to achieve international cooperation in the area of the ICT Trust and Security community.

The BIC project holds an Annual forum for the IAG and this report contains a summary of the Annual Forum held on 27th November 2012 in Lisbon, Portugal.

2. Aims and Objectives

The BIC project's IAG Annual Forum for 2012 comprised two elements:

1. BIC International Advisory Group (IAG) workshop held on the morning of 27th November 2012.

2. BIC IAG Workshop on international cooperation covering trust management for mobile and cloud based services during the afternoon of 27th November 2012.

The objectives of the full day event were:

- **Review of topics under consideration in the BIC Working groups:** WG1. Human oriented/citizen approaches for trust, privacy and security; WG2: Network Information Security / cyber security; and WG3: Programme and funding focus.
- **Identification of 'hot' topics and future work Items for WGs:** To highlight the topics already under discussions in the work groups of BIC and provide input towards future work items for WGs.
- **Identification of country wise Projects and Research Priorities:** Each country was given the opportunity to present the projects, directions and portfolios of research priorities, emphasis and growth areas of interest where international cooperation is an imperative e.g. trust and security, highlighting some recent examples.
- **Identification of tangible Project/Programme mechanisms:** To work out a clear and well defined mechanism to manage projects and programme with an emphasis on fostering meaningful international cooperation (for short term and longer term impact).
- **Identification of Success Metrics:** The BIC workshop in June 2012 brainstormed on the identification of meaningful success metrics for international projects (see section 5). These were presented and the IAG members provided inputs with their own views.
- **Establishment of the BIC/ IAG Structure with Long Term Perspective:** The initial proposed structure from the workshop held in June 2012 [4] regarding a longer term multi-lateral strategy was presented and discussed with the IAG members. As this structure is for a longer term and would extend beyond the lifetime of BIC to be fully up and running (more geared towards H2020), this IAG meeting was extremely important as a planning instrument to further develop the model, and to gain support from a number of exemplar countries that would be willing to take the lead in the establishment of the proposed structure as an inducement to other countries to also participate. It would also provide an early opportunity to identify any barriers to participation.
- **Defining Modalities of EWGs & SFGs**: Evolution of the new modalities for oversight of Extended Working Groups (EWGs) and Special Function Groups) at the participating countries level by the IAG could be a key theme besides defining a roadmap to achieve Key Performance Indicators (KPIs) as derived from an agreed success metric. This aspect has to factor the sanctioned life (36 months) of the BIC project until the end 2013 and desirability of carrying forward after this and aligning with the H2020 vision, whilst finalising recommendations for EC. The structure and relationship of the CWG, EWGs & SFGs with regard to IAG, as presented first at the June workshop and refined at the BIC IAG Annual Forum, can be best understood through the IAG/WGs structure diagram in Figure 1 below.

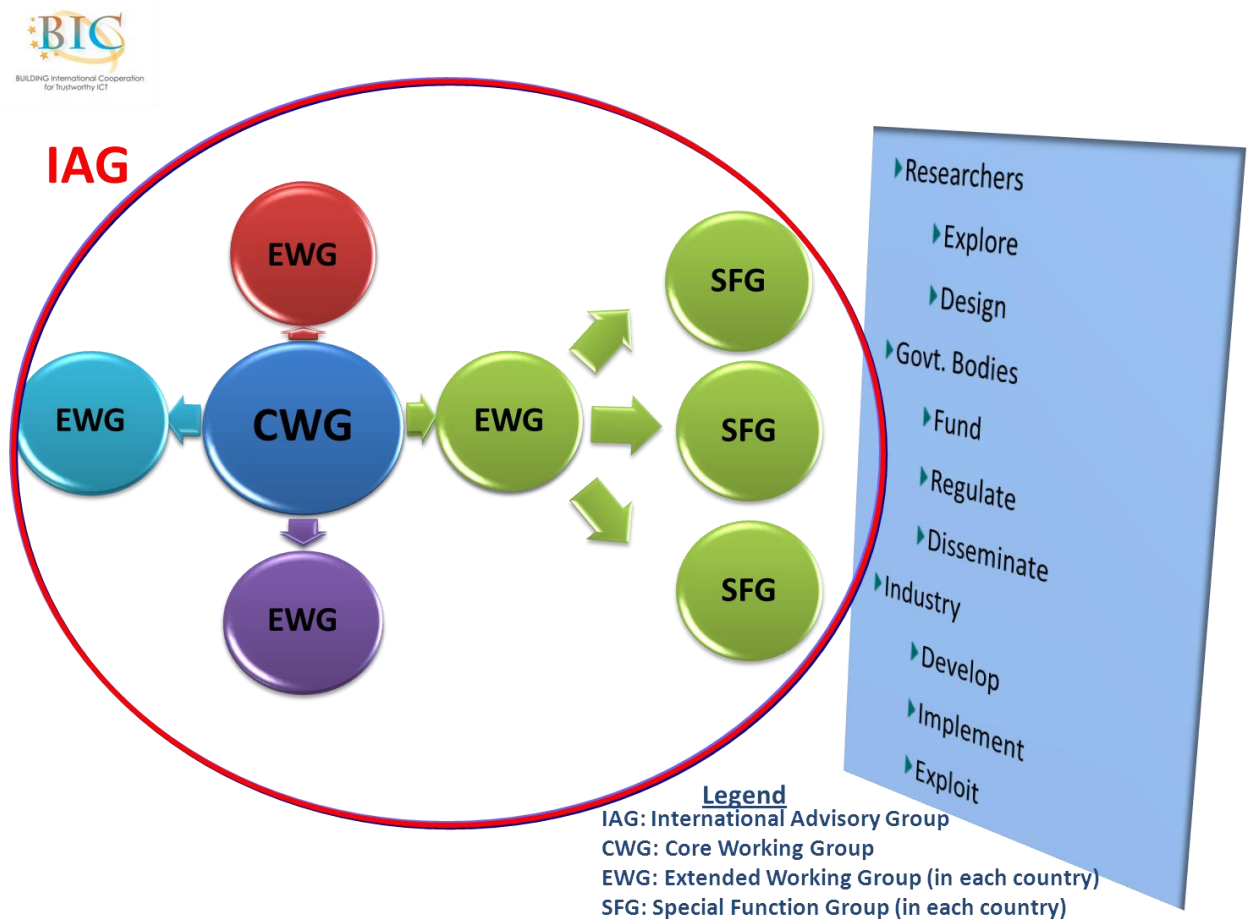

Figure 1- Basic IAG/Working Groups Structure

- **Examination of trust management models in different contexts and cultures** and determining the mutual benefit for international cooperation: Analysing differences, commonalities, synergies between the trust models based in the western world and emerging countries with a view to collaboration; Discussion of the impact on various technologies including mobile and cloud infrastructures in order to support and grow business ecosystems; Identification of on-going projects and the building of tangible project ideas forming; and Next steps – way to move forward on this topic.

3. BIC Working Groups

3.1 Summary of the BIC WGs workshop – June 2012

The first face to face workshop of the BIC working groups was held on 21-22nd June 2012. Since then, there were additional discussion papers received and a full report written of the results [4]. These discussion papers can be found at the project's web portal in the project impact section[1]. Herein contains a summary of the key points from the WGs workshop that were presented at the BIC IAG Annual Forum 2012 in Lisbon by the Work Group leaders:

- The emergence of new threats and new vulnerabilities with new architectures (e.g. clouds), new usages (e.g. social networks), and massive mobility applications (mobile applications within Smartphones) and huge multimedia exchanges (generalisation of music and video flows);
- The obligation of an international cooperation to exchange cyber security data and intelligence to fight against borderless attacks;
- The reinforcement of coordination in cryptography application at the European level to develop robust algorithms for the new usage (enhanced privacy, massive exchange in core networks, mobile e-commerce).;
- The massive emergence of Smartphone applications with new vulnerabilities and future attacks;
- The requirement of a better resilience for critical infrastructures and the enhancement of specification and dissemination for crisis management procedures and tools.
- The new situation of computer science application in computing, storing and communication with the virtualization phenomenon which erases the notion of space and boundaries, making more difficult indeed impossible the legislation enforcement at the country level;
- The reinforcement of digital identity at the global scale, requiring more efforts to protect privacy of individuals and enterprises.

The following topics were particularly highlighted for international cooperation:

- ***New architectures***
  The emergence of new threats and new vulnerabilities with new architectures (e.g. clouds), new usages (e.g. social networks), and massive mobility applications (mobile applications within smartphones) and huge multimedia exchanges (generalisation of music and video flows).
- ***Borderless ecosystem***
  The obligation of an international cooperation to exchange cyber security data and intelligence to fight against borderless attacks.
- ***Scientific cooperation***
  The reinforcement of coordination in cryptography application to develop robust algorithms for the new usage (enhanced privacy, massive exchange in core networks, mobile e-commerce).

[1] http://www.bic-trust.eu/project-impact/

- ***Mobile world***
  The massive emergence of smartphone applications with new vulnerabilities and future attacks.
- ***Critical infrastructure protection***
  The requirement of a better resilience for critical infrastructures and the enhancement of specification and dissemination for crisis management procedures and tools.
- ***Cloud computing - virtualisation***
  The new situation of computer science application in computing, storing and communication with the virtualization phenomenon which erases the notion of space and boundaries, making more difficult indeed impossible the legislation enforcement at the country level
- ***Identity, Privacy***
  The reinforcement of digital identity at the global scale, requiring more efforts to protect privacy of individuals and enterprises.

Taking into account the results of this WGs workshop and subsequent position papers received, the BIC Working Groups current status were summarised as follows at the BIC IAG Annual Forum.

3.2 WG1. Human oriented /citizen trust, privacy and security

According to the terms of reference of the BIC Working groups [5], the scope of WG1 is the following:

- move from the traditional technology-only oriented design of solutions towards user-centric security management; and
- bring together experts from psychology, social science, economics, legal, technologists and trust and security experts to address trust, privacy and security from the point of view of the users, and place them at the heart of solutions.

At the end of the second year of the BIC project, the following topics have been identified by WG1.

Human values

International cooperation allows a dialogue on the expression of multi-faceted human values (freedom of expression, privacy) and their projection into the ICT field.

Cooperation makes possible a dialogue and a mutualisation to express, in computer terms, the practical implementation of these human values on the digital field, such as questions of observing the behaviour of individuals, sovereignty over their personal data, monitoring of internet, etc.

Privacy and Data protection

International cooperation is required to stop the erosion of privacy that is currently happening. The questions that need to be discussed in order to stop the erosion of privacy are:

- Who is responsible for the preservation of an individual's privacy? Is it the government? The corporations? Or the responsibility of the individual?
- How can we as a research community empower the individual to take control of his or her own private data?

- What new powers are needed by the governments to restrain the “privacy violation industries”?
- How can corporations be convinced of the added value provided by privacy preserving services (see the ENISA report on the Monetization of Privacy [17])?

Data provenance

When we see data on the Web, currently, we do not know where it came from and how it got there. This information and its source (provenance) is typically lost in the process of copying/ transcribing/transforming databases. International research communities should work together to ensure that data provenance provided as an essential attribute to ensure data integrity, currency and reliability.

Trust

International cooperation allows everyone to share different trust models in order to implement trust infrastructures (protocols, architectures, services) to reassure users (citizens and businesses) in their daily lives.

The cooperation enables a discussion on the various choices, based on cultures and customs, of the notion of trust that will evolve over time, as habits change and maturity of digital users grows.

Social computing

Social Computing enables user-centric, collaborative knowledge sharing to build communities of people using the Internet. When Social Computing emerged around 2003, it was not thought that a few years later millions of users across the world would be using Social Computing applications such as online social networks, blogs, collaborative filtering of content, and many more. Social computing supports social behaviour with computational systems by recreating social conventions and contexts using technology. At a more technical level, Social Computing is supported by technologies such as collaborative filtering, online auctions, and reputation systems and social network analysis. There is great value in Social Computing systems as they are empowering users and driving the creation of new digital divides. Social Computing is a driver for growth and employment, is disrupting many industries and has the potential to reshape work, health and learning.

Designing identity management and accountability frameworks

Identity is still a concept largely national and cultural. In the 2000s, identity infrastructures have just been digitised similarly to what already existed on paper. International cooperation is crucial to redefine digital identity at the international level (or at least continental with international interoperability), so that legal and liability issues are resolved at the root, that is to say to the identifying subjects and objects.

Cybercrime

International cooperation is to pool the efforts of various countries together to fight against cyber crime and attacks.

Cooperation to share more information and to interconnect alert systems enables a faster response to future propagation of attacks around the world.

3.3 WG2. Network Information security / Cyber security

According to the terms of reference of the BIC Working groups [5], the scope of WG2 is concerning network security, in general: security of infrastructures, systems, services, components, devices. WG2 focus is on the following topics:

- International data exchange architecture for cyber security;
- policies relating to how the collected cyber-intelligence is to be handled, exchanged, shared and utilised;
- Open source trustworthy host platform for collaborative research and education;
- International cooperation in Cryptology;
- Mobile security of software services;
- The planning and improvement of joint exercises related to cyber security across borders.

At the end of the second year of the BIC project, the following topics have been identified by WG2.

Securing the current and future Internet related to diversity, complexity and interoperability

International cooperation is currently inadequate for today's Internet to address its shortcomings and to fight against cybercrime, which benefits from technical legal vacuum to use to his advantage the lack of tools for tracking in real-time international crime in various countries.

International cooperation is must at the outset of the Future Internet to be widely used, so that everyone is consulted to ensure that new architectures and new protocols can take into account a global vision of the network.

New privacy infrastructure, reconsidering privacy spaces, storage function and container-isation?

The private sphere is largely disrupted due to the centrifugal force of personal data that are pushed to the edge of networks, and this, willingly or unwillingly, very often unknown and beyond the control of individuals.

International cooperation on a deep reflection on data storage, on content exchange is essential to restore the private territories and to preserve private behaviour of every citizen in the digital ecosystem, so that citizens do not feel observed in their digital behaviour, and their location in their daily commute, and that their data are not placed in the open, available to everyone. International cooperation must also consider the erasure of data and the right to oblivion, so that certain digital traces cannot ever harm the citizens.

Cryptography

Advanced cryptographic protocols are needed to support privacy and user control in the cloud and in the Internet of things; as these two worlds need to interoperate, key goals are the development of functional encryption, the distribution of secrets to avoid single points of failure, the optimization of dedicated multiparty protocols and the development of novel protocols based on tamper resistance. Cryptography has a key role to play in the developments of privacy-by-design, and in applications such as metering, subscriptions, information sharing and data retrieval. A particularly challenging and high-impact application is e-voting.

Mobile Security

Significant work is going on across the globe to address threat to the mobile security and associated entities. More collaborative efforts are required in a highly organized manner to achieve the maximum output of all those efforts and to derive the best possible results optimally. The coordination and collaboration is required to Create a Centralized Body (like ITU) who shall Formulate Regulatory Policies, define Standards, Tools & Test Beds, organize Coordination amongst different scattered research bodies and entities involved in developing mobile security measures and apps, organize consolidation and compilation of available and ongoing work and organizing their development and dissemination through industry sources.

Software security

International cooperation is important in software security, because software security research is too dispersed. While software engineering (formal methods, software correction, software assurance methods of compliance) has many international conferences, research on methods of detecting dangerous levels of software (dangerous viruses, detection of dangerous software) is orphan, too compartmented and very secret. This research should be open and become an academic discipline, as this was the case of cryptology, twenty years ago.

Standardization and derived metrics

International cooperation is natural and widely developed to standardize emerging technologies. However, this recommendation is to renew the security methods, tools and variables to measure. These are primarily international reflection to implement new concepts, new recording and measures (for trust, logs, etc.), for the Future Internet.

This standardization and research on these metrics must be done before the deployment of technologies.

International cooperation is natural in this field of standardization (methodology, benchmarking and standards) and long-term research on scientific grounds (cryptology).

Digital forensics

Digital forensics analyses needs to be truly adapted to the virtual world of a digital ecosystem. New methodologies and tools need to be developed to meet the requirements of performing digital investigations of cyber world. These new techniques need to consider the peculiar characteristics of virtualisation of computing and storage resources besides globalisation of criminals and their targets.

Securing cloud computing for enterprises

International cooperation is essential for large companies with an international dimension to specify their requirements in security and irreversibility of service in the cloud, so that each client can take control of its information. When failures occur (disappearance, failure, loss, shift, merge or sale of a cloud service), the technical and legal problems may be serious and will impact all economic and technical architectures with transcontinental virtualization tools.

Initiate green security

International cooperation can expand the concepts and vision of a new security. The environmental considerations are not only at the power consumption of equipment and saving paper. International cooperation can provide some thoughts on new architectures and new ways of understanding security as a whole.

3.4 WG3. Programme /funding focus/ identify community

The terms of reference of BIC Working Groups [5] specify that WG3, (Programme/funding and focus/identify community,) will focus on a multi-disciplinary approach towards establishing international cooperation (INCO) between all stakeholders.

During the past year of the BIC project, there was a significant ramping up of the strategic component of the project via Working Group 3, and delivering significant progress on developing a long term strategy for international cooperation in the EU RTD programme in conjunction with international parties around the globe.

The BIC project has taken a lead role working with the communities engaged with INCO towards reflecting on a longer term strategy for international cooperation. To this end, the project organised a joint workshop across the International relations Unit D.1 and the Trust and Security Unit H.4 entitled *Cross domain coordination of International Cooperation and technical themes in Trustworthy ICT and INCO* in June 2012 and during this two day workshop, a large number of international cooperation (INCO) projects[2] brought their insights and European Commission participated [4]. At this workshop, WG3 had a full day dedicated to exploring the insights and common experiences across a large number of INCO related projects and identifying, discussing and assessing (a) key challenges, issues and priorities; (b) mechanisms for international cooperation that are already available; and (c) identification and determination of 'success metrics' for INCO. A member of the BIC IAG, Mr. Abhishek Sharma presented an initial draft of a long term 'strategic approach' for international cooperation in trustworthy ICT and this led to very interesting discussions and feedback.

This 'strategic thinking' approach towards international cooperation has also been mirrored in the European Commission's presentation (see section 4.1) regarding international cooperation approaches for H2020 during the programme management session of the BIC IAG forum 2012 and subsequently at the EU-Africa ICT Forum plenary session the following day [18].

Taking on board the comments and discussions from the June Workshop, Mr. Sharma presented the BIC approach developed in WG3 during the programme management session. The IAG members present agreed that proposed approach is a good way forward and they will promote it back in their countries. It was also agreed that since the approach required additional structures above and beyond the scope of BIC, it was important in the next year for the IAG to begin to discuss ways to address this after the conclusion of BIC.

[2] **IST Africa, EuroAfrica-P8, FEED, AUS-ACCESS4EU, PACE-Net, EU– India Spirit, Synchroniser, OpenChina-ICT, SECFUNET, FIRST, FORESTA, PAERIP, SEACOOP, AMERICAS, and IST-EC2.**

3.5 Discussions on topics for International cooperation

During the animated panel discussions sessions, the focus was on whether the Working groups of BIC were on target and/or whether particular topics required additional attention. A number of IT trends were identified as requiring further attention for international cooperation in security. The main points were the following:

- **The constant digital integration by widening and deepening in the ecosystem creates new source of new vulnerabilities.**

The digital ecosystem will continue to be deployed in many sectors, and for more populations, and will continue to deepen in every domain of human activity.

For international cooperation, the digital ecosystem is not limited to the Internet, mobile phones and television. It is also important to consider the geo-navigation services, the future smart grid services, logistics (RFID, NFC), the movement of goods and people and the entire industry of hardware and software in general. This constant integration of new sectors and the permanent opening to new horizons offer new breaches for international cyber-crime and for any trans-boundary failures, with cascading effects. International cooperation on critical infrastructure protection and crisis management is crucial to reassure users' confidence and to ensure service continuity of socioeconomic activity.

- **International cooperation needs a long-term vision with humanistic values and appropriate governance.**

This digital ecosystem requires a long-term vision and a control adapted to the challenges posed by the opening of global markets on the one hand, and the permanence of a rule of law applicable in this area, through internationally harmonized legislation, on the other hand. But cooperation should aim to offer as a worldwide vision of the future digital ecosystem, with its opportunities and threats for Europe and the world in general. This new space cannot be deployed and cannot be operated without controlled governance and without reference to humanist values.

Properties of the ecosystem include respect for diversity, plurality of architectural models and economic models, the ecosystem resilience, the neutrality of the whole digital ecosystem, not just the internet, everyone's responsibility stakeholders (providers of content and services, telcos and cloud computing, users, etc..), the creation of cultural common, the preservation of intellectual property of creators, the remuneration of authors the digital sovereignty and digital dignity of responsible users (citizens and businesses).

- **International cooperation should anticipate the new features of the ecosystem with their security requirements.**

The economic value and the social power of digital activity will grow in this expansion and this deepening ecosystem. Resilience of infrastructures and large systems is a necessity for daily activity of individuals and businesses.

The digital space is also becoming more flexible (elastic cloud computing) and more accessible through virtualization techniques (resources of storage, communications, computing, services and software, available on the network, at any time, by individuals, businesses, institutions). This exacerbated dynamicity

creates new vulnerabilities onto these systems: resistance to adaptivity, scalability and reconfiguration is essential.

But Internet, mobile telecoms, IT and digital industry remains essentially a software industry. The control of its foundations (language theory, design and manufacturing of applications) and mastering the software life cycle (innovation, design, development, deployment, evolution, maintenance, obsolescence, destruction) remain the basic of digital system trustworthiness. An overhaul of the theory of vulnerability and dangerousness of software, and a review of security and robustness of software is required.

Usage of software causes far-reaching effects. This usage is facing more frontally sociocultural, political and economic reactions, which greatly influence its evolution often slowing and sometimes accelerating security measures that we would implement at the international level. A greater obligation on robustness, security and privacy services, from software editors, is probably essential for the implementation of large-scale services.

- **International cooperation should envisage to constantly revisit the new forms of worldwide cyber violence.**

This space of expression and freedom also has its setbacks. Violence in all its forms (crime, fraud, malevolence, slander, defamation, activism, exacerbated expression, trade harassment ...), is an intrinsic part of our civilizations. It creates confusion, but also sometimes helps to establish a new order in a destabilized digital evolving world.

We must distinguish, in this digital changing world, technological violence of technique and practice transformation, which generates innovation, usage evolution, and malicious violence (greed, unfair attack of competitors), that is harmful to all stakeholders (users, service providers, operators), in connection with crime and malicious behaviour.

International cooperation should intervene on physical elements (equipment, software, data), but also on societal behaviours (reputation) with actions that affect the educational, sociological, ethical facets.

4. Programme Management session

The programme management mechanisms and stakeholders of the BIC countries were represented.

4.1 Europe

The BIC Annual forum was quite timely as the Commission unveiled a set of proposals in November for Horizon 2020 (H2020), the new framework programme for research and innovation. This forms part of the set of proposals for all of the Union's spending programmes for the period 2014-20.

The H2020 programme responds to the economic crisis investing in future jobs and growth. It is addressing peoples' concerns about their livelihoods, safety and environment and strengthening the EU's global position in research, innovation and technology.

In terms of the rationale for (What for?) and with whom? (country fiches), in H2020, the Commission is adopting a "strategic thinking" and the BIC report from

the June 2012 workshop [4] was singled out as providing some useful material for this aspect. The approach would take into account the issues being raised by BIC and other INCO related projects, European ICT platforms, IPR, standards, instruments and cover key areas of the Future Internet, Cyber-security, micro and nano-electronics, sensor network, enterprise software, urban environments and e-mobility, trust and security. Included in this would be international cooperation with industrialised countries, BRICs, developing countries, amongst others.

INCO for ICT research and innovation in a globalised world was covered in the ISTAG report, which had a number of recommendations:

- Reinforce policy dialogue with 3rd countries developing a more articulated view of policies dealing market access, research and innovation;
- A more sophisticated view of “mutual benefits” – go beyond “reciprocity” in mutual research programmes;
- Safeguarding intellectual property rights is key but this should not result in excluding international partners from the possibility to exploit foreground IP;
- Simplifying “joint calls” and look for more agile forms of collaboration;
- Further develop collaboration with labs outside EU, in technological research as well as take-up and deployment (test-beds, pilots).

To find out more information about the transition to Horizon 2020, please visit http:// www.ec.europa.eu/research/horizon2020.

Also, visit the site on International Cooperation for lasting solutions http://ec.europa.eu/research/iscp

Current Mechanisms

As a number of the current mechanisms from FP7 are envisaged to still be available in Horizon 2020, the European Commission presentation concluded with how the European Commission’s Framework programme 7 (FP7) has supported international cooperation, including those within areas related to trust and security research, in a number of different ways.

The first is a ‘**general opening**’, where international partners are welcome to participate in all Challenges and Objectives with the following eligibility criteria:

- Minimum 3 different EU Member States or Associated Countries
- Beyond this minimum, all non-EU/non-AC countries can participate

The second is a ‘**targeted opening’**, where the participation of third countries is particularly encouraged. The targeted openings are explicitly mentioned in some of the Objectives (e.g. Australia, South Korea under WP2013).

The third is part of ‘**Horizontal Actions’** including bi-lateral coordinated calls. Some examples include the coordinated calls with Brazil and Japan (under WP2013) and international partnership building and support to dialogues (Objective 10.3 under WP2013).

A number of targeted openings in WP2013 were highlighted during the workshop including:

1. **Objective ICT-2013.1.5 Trustworthy ICT:** EU-Australia cooperation on building user trust in broadband delivered services
   - Demonstrate in a real-life environment the maturity and practicality of a digital authentication framework in broadband delivered services working across several jurisdictions (organisational, governmental) with high levels of assurance.
   - Funding: up to €3 million
2. **Objective ICT-2013.1.7** Future Internet Research Experimentation (FIRE):
   - EU-South Africa cooperation on future internet experimental research and test-bed interconnection
   - EU-China cooperation on future internet experimental research and IPv6
   - EU-South Korea cooperation on future internet experimental research
3. **Objective ICT-2013.2.2** Robotics Use Cases and Accompanying Measures:
   - Robotics networking -help identify new users and markets and new research areas through sector-based analysis; establish a strategy towards sustainable international cooperation in robotics, focussing initially on the United States.

A number of coordinated calls available in WP2013 were highlighted.

1. ICT-2013-10.1-EU-Japan Research and Development Cooperation. A number of important events have taken place between the European Commission and EU research communities with Japan (MIC/NICT) over the last few years in the “Future Internet” domain. This work has led to the organisation of an EU-Japan coordinated call that is part of the research Work Programme 2013.

The topics for consideration include:

a) Optical communications
b) Wireless communications
c) Cybersecurity for improved resilience against cyber threats
d) Extending the cloud paradigm to the Internet of Things – Connected object and sensor clouds within the service perspective
e) Federation of test-beds: control, tools and experiments
f) Green and content centric networks

The funding scheme for the coordinated call with EU- Japan is Small or medium scale focused research projects (STREPs) with an indicative budget of EUR 9 million (a similar budget for the call is expected from the Japanese MIC and NICT). The timing for the call is 2 Oct – 29 Nov 2012.

The whole work programme is subject of an information day in Warsaw, Poland on 26 and 27 September 2012. See information at: http://ec.europa.eu/information_society/events/ictproposersday/2012/index_en.htm.

In addition, concerning the EU-Japan R&D activity, a dedicated page has been opened where you can submit your ideas, partner search, and take this opportunity to be part of the EU-Japan networking session that takes place on 27 September 2012. You will find the relevant additional information at:

http://ec.europa.eu/information_society/events/cf/ictpd12/item-display.cfm?id=8435

2. ICT-2013.10.2 EU-Brazil Research and Development Cooperation. The topics for consideration include:

   a) Cloud computing for Science;

   b) Sustainable technologies for a Smarter Society;

   c) Smart Services and applications for a Smarter Society ;

   d) Hybrid broadcast-broadband TV applications and services;

The funding scheme for the coordinated call with EU - Brazil is Small or medium scale focused research projects (STREPs) with an indicative budget of EUR 5 million (a similar budget for the call is expected from the Brazilian Ministry of Science, Technology and Innovation (MCTI). The timing for the call is 10 Jul – 24 Oct 2012.

NOTE: The deadline for ICT-2013.10.2 EU-Brazil Research and Development Cooperation call has now been extended until 7th February 2013 and more information can be found at https://ec.europa.eu/research/participants/portal/page/cooperation?callIdentifier=FP7-ICT-2013-EU-Brazil#wlp_call_FP7

The Horizontal International cooperation actions available in WP2013 include Objective ICT-2013.10.3 International Partnership Building and Support to Dialogues, where the goal is to support dialogues between the European Commission/the EU and strategic partner countries and regions, and to foster cooperation with strategic third country organisations in collaborative ICT RTD both within the EU's Framework Programmes (FP7, Horizon 2020) and under relevant third country programmes. The Targeted countries/regions include:

   a) ACP countries (in particular Africa)

   b) Asia (in particular China, India, South-East Asia)

   c) Eastern Europe and Central Asia

   d) High Income Countries: Subgroup 1: North America (Canada, USA)

   e) High Income Countries: Subgroup 2: East Asia/Oceania (Australia, Japan, Korea, New Zealand, Singapore, Taiwan)

   f) Latin America

   g) Mediterranean Partner Countries

It is expected that each targeted area will be covered by at least one project, and that duplication of effort in an area is avoided. The Funding scheme/expected budget is Coordination and Support Action (CSA) (SA) with €8 million (maximum EU grant of EUR 800 K per proposal). The date of publication of Call 10 is 10/07/2012, call deadline: 15/01/2013.

4.2 Brazil

The BIC IAG members consist of members from two of Brazil's funding agencies for ICT, including trust and security related research. These include:

- CNPq and FINEP (financiadora de estudos e projetos) have public calls for funding. These are national foundations linked to the Ministry of Science and Technology. More information at http://www.cnpq.br/english/cnpq/index.htm and http://www.finep.gov.br/english/FINEP_folder_ingles.pdf.
- CTIC is the Research and Development Centre for ICT of the Ministry of Science and Technology. They are an alternative to CNPq but with more of a focus in ICT. Currently, they have several funding lines, one in DigitalTV, another in Cloud Computing, another in Smart Cities and another in Network Virtualization. Website can be found at http://www.ctic.rnp.br/.

As an example of a successful international targeted call involving a security element, the recent Brazil – EU call was highlighted. In September 2010, the CNPq of Brazil and DG INFSO of the European Commission launched a coordinated call for bi-national projects in ICT with the total amount of R$ 11million/ 5 million Euro, with up to R$ 3 million/1.5 million Euro per project. Five areas were included in the call (Edital CNPQ No. 066/2010): Future Internet - Experimental Facilities, Future Internet – Security, Networked Systems and Control, e-Infrastructures and Microelectronics/Microsystems. But only one project per area were able to receive the budget.

As a result to this call, a range of research groups in Brazil and EU had the common objective to promote interaction and cooperation, but for many research groups in Brazil it was the first experience of preparing a project proposal with FP7 requirements and format. Nevertheless, several consortiums were formed, but not so many achieved the coordinated project submission.

Lessons have been learned with the coordinated project submissions, mainly considering that the coordinated call is fundamental to have a formal means to promote cooperation between researchers from European and Brazilian communities. More specific calls to Future Internet and related topics would stimulate more projects, and encourage consortiums to improve the quality and experience of the partners.

As mentioned above, within WP2013, there is another ICT-2013.10.2 EU-Brazil Research and Development Cooperation. The topics for consideration include:

a) Cloud computing for Science

b) Sustainable technologies for a Smarter Society

c) Smart Services and applications for a Smarter Society

d) Hybrid broadcast-broadband TV applications and services.

NOTE: The deadline for ICT-2013.10.2 EU-Brazil Research and Development Cooperation call has now been extended until 7th February 2013 and more information can be found at https://ec.europa.eu/research/participants/portal/page/cooperation?callIdentifier=FP7-ICT-2013-EU-Brazil#wlp_call_FP7

4.3 South Africa

The key funding bodies/programmes in South Africa are the following:

1. Dept of Science and Technology (DST) – http://www.dst.gov.za engages in mostly institutional funding eg to science councils like the Council for Scientific and Industrial Research (CSIR) http://www.csir.co.za/, space agency, and large science initiatives like Square Kilometer Array.
2. DST - EU-South Africa Science and Technology Advancement Programme (ESASTAP) (http://www.esastap.org.za), which provides seed funding for proposals, National Contact Point funding, co-funding of FP7 projects and COST travel funding.)
3. DST - Technology Innovation Agency - http://www.tia.org.za provides funding for development and commercialisation.
4. NRF, National Research Foundation - http://www.nrf.ac.za provides funding for schools, university research, research chairs, furthering education, and international bilateral S&T programmes.
5. NRF - THRIP = Technology and Human Resources for Industry Programme in collaboration with Dept Trade & Industry, http://thrip.nrf.ac.za provides funding for industry based programmes.
6. SPII - support programme for industrial innovation (Dept of Trade & Industry) - www.spii.co.za
7. eSkills Institute as part of the Dept of Communications -http://www.doc.gov.za provides internal funding for eLearning and eSkills programmes.

The DST, along with the IAG members from the CSIR Meraka Institute, SAP Research Pretoria and University of Pretoria have been particularly supportive of the BIC IAG and working groups. In addition, a number of other African countries (Tanzania, Kenya, Malawi, Ethiopia, Sénégal) participated to the BIC IAG Annual forum and they are very welcomed to continue participating within the current structures.

4.4 India

The main funding agency responsible for funding Research and Technological Development (RTD) in India is the Department of Information Technology (DIT), which falls within the Ministry of Communications & Information Technology of the Government of India. The units in DIT dealing with all areas of ICT trust and security are described below.

The Cyber Laws & eSecurity Group, as shown in Figure 3**,** contains a number of different programmes:

- Cyber Security strategy [6] - A cyber security strategy has been outlined by DIT to address the strategic objectives for securing country's cyber space and is being implemented through the following major initiatives: Security Policy, Compliance and Assurance; Security Incident Early Warning & Response; Security training skills/competence development & user end awareness; Security RTD for Securing the Infrastructure, meeting the domain specific needs and enabling technologies; and Security Promotion & Publicity.
- Cyber Laws strategy [7] - Provides legal recognition to electronic documents and a framework to support e-filing and e-commerce transactions and also provides a legal framework to mitigate, check cyber crimes.
- Cyber Security R&D strategy [8] – promotes research & development activities through grant-in-aid support to recognized autonomous R&D organizations and academic institutions proposing to undertake time-bound projects in the thrust areas identified.

The closest to Unit H.4 Trust and Security within DG-CONNECT of the European Commission [9] would be a combination between the Cyber Security strategy and Cyber Security R&D groups, probably more so towards the latter. The DIT mainly funds research and academic institutions. There are other programmes that may also touch upon some of the other topic areas covered in the EU including one dealing with judicial matters in relation to Cyber space, the Cyber Appellate Tribunal (CAT[10]); Indian Computer Emergency Response Team (ICERT[11]), the nation's referral agency of the Indian Community for responding to computer security incidents as and when they occur; and Controller Of Certifying Authorities (CCA[12]), provided for by the Information Technology Act, 2000 [13] as the governing authority which licenses and regulates the workings of Certifying Authorities [14], who issue digital signature certificates for electronic authentication of users.

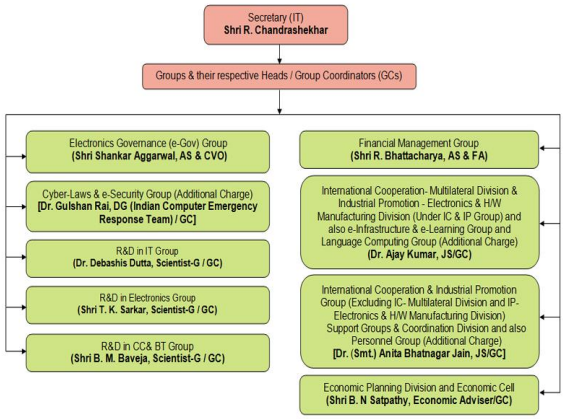

Figure 3. DIT Groups and their respective Heads/Group coordinators [4]

With regards to International cooperation and how it links to Trust and Security, there is an International cooperation Directorate that works very closely with the Directorate under which the Cyber Security and eSecurity group belong. There are a number of departments related to international cooperation and the most appropriate one for Trust and security research would be the Department of International Cooperation & Industrial Promotion, Bilateral Trade Division [15]. There are already a number of FP7 projects engaged in EU – India cooperation (e.g. ERNET India connectivity with European Research Network – GEANT) and these are detailed at [16].

How funding or R&D projects in Cyber Security Works

Department of Information Technology (DIT) invites R&D project proposals in Cyber Security area. Cyber Security R&D initiative of DIT in an open call fashion that is aimed at promotion of basic research, technology demonstration, proof-of-concept along with indigenous development of technology in the area of Cyber Security [16].

The Cyber Security Programme also includes establishment of test bed projects for enhancing indigenous skills and capabilities.

As detailed above, the main thrust areas of research and development identified include (a) Cryptography and cryptanalysis, (b) Network and systems security, (c) Security architectures, (d) Vulnerability and assurance and (e) Monitoring, surveillance and forensics.

R&D proposals are invited from autonomous academic and R&D organizations in the following specific areas: (i) Mobile Security, (ii) Malware detection and analysis, (iii) Network and system security assurance, (iv) Cryptography and cryptanalysis, (v) Monitoring tools for network and system security, (vi) Enterprise forensics and (vii) Mobile forensics.

The proposals may be single or multi-institutional, with clearly defined milestones/timelines and role of individual institution. Project proposals duly endorsed by the institution (in 25 copies in prescribed format enclosed) may be sent to Member Secretary, Working Group, E-Security Division, Department of Information Technology, Electronics Niketan, 6 CGO Complex, Lodi Road, New Delhi -110003.

5. Trust Management for emerging countries

During the BIC workshop in June 2012, one of the Working group sessions (WG1) held discussions on various trust aspects and how research between the EU and the emerging countries could enlighten more on potential solutions for trust management [4].

Trust models implemented in currently available technology is developed based on the principals of trust as a social phenomenon within the context of the western world. Indeed, the majority of the research on these topics has come from westernized or individualistic cultures, where consumer trust is facilitated through trust mechanisms such as institutional guarantees, laws and policies, information security mechanisms, and social controls. Examples of this way of trust formation are finding evidence of the number of positive experiences and recommendations between entities in a trust community.

This is in contrast with trust formation in other cultures, e.g. Africa, Asia, India and South America, where structures embedded in the society are much more relevant. Consider, for example, the important impact that a person's ethnic relationship (collectivist) in Africa has on the formation of trust. Therefore, the principle of similarity from a societal point of view can be considered as one of potentially many different and important parameters in building trust models that are also of relevance to the developing world.

With the proliferation of mobile technology within these emerging countries and the impetus it has already given to the formation of innovative business models, such as virtual co-operative buying ecosystems, there is already an acute need for technology that will instil trust within the user community. For example, the user community in Africa is characterized by small to very small enterprises conducting their whole business from a mobile phone. The international research results to be delivered by this initiative should, therefore, aim in conceptualizing trust mechanisms that operate seamlessly in a mobile-cloud infrastructure.

It is, therefore, possible that we can find topics of mutual interest to collaborate on, as it is of interest not only to those in the African context, but to any environment where different types of cultures exist, and where an understanding of the influence of culture on trust is limited. Considerable amounts of research still has to be done on identifying the unique properties/requirements related to trust used by people in collectivist cultures and how this can be captured by mobile technologies in order to support and grow business ecosystems.

During the BIC open workshop held on the afternoon of 27th November 2012, the concentration was on this research topic to put us in a better position to form consortia that can work on research/development/implementation/ stages for this work. There were a number of participants showing particular interest in this area, especially from Africa, India and the EU and are already discussing the potential for setting up a consortium on the topic. Further information can be found in Annex 1, section A1.3.

If you are involved in this research topic from any perspective and are interested to take it further within this group, please send a one page position paper on this topic to jclarke@tssg.org.

6. Success metrics / Impact evaluation

One of the main coverage areas of BIC is the determination and identification of "success metrics" for international cooperation and collaboration. Work on this was initiated at the June 2012 BIC workshop [4] and the results from that workshop were presented during the BIC IAG annual forum (for completeness, the full version can be found in Annex 2).

At the BIC Annual Forum, it was suggested that there was a need to clarify the aim of this exercise as there was some initial confusion at the June workshop about the applicability of criteria for success metrics, whether the focus should be on individual project(s) or the programme as a whole.

This point was addressed and during the discussions during the IAG session and it was clarified that the criteria for success metrics would indeed be at the programme level and not at the project level. However, this would then be broken into other sub – levels such as:

- **Research and Technological Development:** mutually beneficial projects' success and impact of results for the participating countries and stimulation and planning of further research needed collectively;
- **Economic and Commercial:** business done, what has been exploited/how, number of companies created, stimulation of new business and enrichment of business environments, sharing and cooperation between industry-led technology platforms, etc.;
- **Knowledge gained:** specifications, new standards, new technologies, sharing and learning new techniques, tools and methodologies, increase in productivity and efficiencies, etc.;
- **Social, Legal and Regulatory matters:** new directives for EU and internationally agreed norms;
- **Programme Development:** progress in removing barriers (identifying and overcoming) for INCO; coordinated / targeted calls created arising from the funded INCO activities (e.g. EU – Brazil, EU – Japan, …).

It was agreed that with these guidelines better defined, more productive time could be spent within WG3 on this topic during the next workshop.

7. Conclusions

The digital industry is a key to growth and competitiveness of enterprises and at the crossroads of education, culture, knowledge and social links thanks to the immediate interconnection to the network. The digital domain has become the real heavy industry of the 21st century. The Achilles heel of this industry is security.

The European Union has taken measures to protect intellectual property, privacy of citizens, to fight against illegal and harmful content circulating on the networks, to promote e-commerce with secure transactions. In summary, a number of areas were highlighted during the IAG workshop as key topics for international cooperation in Trustworthy ICT.

- **Cyber crime and cyber forensics**

Despite the initiatives, the U.S., Europe and various continents, cybercrime has a tendency to grow and requires an international response that must include all countries without exception. The major issue of universal consensus on the threat of cyberspace is not yet established and comprehensive measures against cybercrime are not really addressed.

- **Identity management frameworks are required for people, multimedia content, Internet of Things**

Crime and fraud is mainly due to the activity value on the Internet (e-commerce, sensitive information exchange). Threat operates essentially identity theft. It is therefore essential to coordinate identity management frameworks for people and also digital assets (IoT, directories, and databases), geo-location frameworks of people and goods (geographic database, database images, etc.).

- **The scope of threats widens towards applications and direct expressions with disinformation, defamation, denigration, e-revolt**

The threat of rebellion, tarnish of the image, of reputation, of dignity of individuals and companies, is mainly due to the new area of freedom (in every sense possible) that allows anyone to expression (knowledge, information, display, lying, disinformation, propaganda, smear ...). The network is a megaphone, a sounding board that allows a small source to assert its presence as the network to defend any interest. Knowledge, information, traffic data are sometimes less important than advertising, rumours, misinformation. Anonymity allows removing censorship in the expression, densification allowing collective actions (syndication flow of thoughts), that dis-empowers individuals.

The network has become an area of interest where industry groups, states, international organizations are strongly involved. Can we regulate cyberspace? Can we think about rules, avoiding censorship on what is said, what is displayed (which is stored), what is exchanged (which is communicated), what is calculated, is created (which is processed)?

- **The spectrum of attack organizations is fragmented and extends with cyber-hacktivism and new stealth attacks, in viral organization**

There is a set of parallel structures between computer architectures and the active militant organizations, rebelling against the established order of official computing business and contributing to hustle and reinvent relationships on the network. In parallel to open architectures (UNIX, Internet) in the years from 80 to 90, there has been the emergence of the free software and open movement. In the years 2000 – 2010, we have seen the emergence of decentralized and peer-to-peer

applications and the later the emergence of virtualization and cloud computing. At the same time, we have seen the coming out of fragmented movements, that are very scattered, covered in anonymity, networking, driven by the same ideology, and flexible to be reconfigured according attack missions against a website or a service provider.

As well as virtualized architectures (peer-to-peer, cloud computing) are increasingly deployed, while being diluted in the mass or hiding their real topology, these more fragmented attack groups appear, either diluted without perimeter or highly organized and secret, wearing the same ideological banner.

Collectives (such as Anonymous) or groups like Wikileaks have similar organizations to new computer architectures. It can be viral organizations as banners that allow people that do not know each other and join their forces conducting one or more actions. Attacks are militant actions, denigration, spontaneous massive appointments, and orchestrated attacks in denial of service or sending mass e-mails.

Table 1 highlights the topics for future WG coverage.

Topic	**Description of INCO topic**
Mobile Security	The massive emergence of smartphone applications with new vulnerabilities and future attacks The emergence of new computer paradigm (virtualization) which tends to dilute space and time creates new vulnerabilities with the difficulty of tracing locations of resources.
Mobile Cloud Computing Paradigm = mobile + cloud security	The new situation of computer science application in computing, storing and communication with the virtualization phenomenon which erases the notion of space and boundaries, making more difficult indeed impossible the legislation enforcement at the country level.
International data exchange architecture for cybersecurity	Policies - relating to how the collected cyber-intelligence is to be handled, exchanged, shared and utilised; and Joint exercises - Planning and improvement of joint exercises related to cyber security across borders.
Identity, Privacy	The reinforcement of digital identity at the global scale, requiring more efforts to protect privacy of individuals and enterprises; and taking into account diversity of cultures. Identity management is valid for persons but also for goods. International cooperation is needed for Identity management frameworks of all sets of digital assets, with all the interoperability issues.
Trust management models	Cultural based trust models e.g. trust models based on collectivist vs. individualist cultures. Trust in data - Information and its source (provenance) is typically lost in the process of transcribing databases. Trust resulting in services that are composed from atomic services, delivered by providers (with different trust scores) Trust based on recommendation and/or reputation for Very Small Enterprises => International cooperation needed to allow sharing different trust models and in order to implement trust infrastructures (protocols, architectures, services).
Security as a Service	**1.** Security risks shifts from the IT system as a whole to the services it offers to a multitude of independent users and to the data that travels across systems

Topic	Description of INCO topic
	2. Security innovation raises new challenges - forensic tools for mobile-cum-cloud; data-centric policies; simple + basic authentication; ecosystem access control policies; privacy-preserving computing; and aggregation of different access approaches. **3.** Innovation provides user-centric approach towards the personalization of security services - most important protocols in ensuring transparency and security within Cloud computing is the SLA - only legal agreement between the service provider and client. **4.** Ensuring mobile and cloud security is still a serious challenge! **5.** For INCO in emerging countries, we should focus on mobility within cloud infrastructures **6.** Construction and usability aspects of the proposed SeciYP platform - An innovative framework for accessing loosely coupled (but interoperable) cloud-based security services by a variety of end-users, in a secure, effective and flexible manner, anywhere and anytime, using their mobile devices.

Table 1 – Topics for international cooperation advocated by the IAG

Having recognized the importance and relevance of International Cooperation in addressing the critical issue of ICT Trust & Security, it is essential to appreciate that the organisation of this level of cooperation needs special treatment to identify and define objectives, work out an effective execution plan, and manage its implementation to achieve the intended results. This is certainly being brought forward in the strategic pursuits of BIC as they are establishing the objectives and managing the different levels of cooperation between the countries, duly taking into consideration the challenges to address. In the past year of BIC (2012), we have made excellent strides in promoting a strategy that is based on the need for the expansion of the current mechanisms to include both bi-lateral (tactical) and multi-lateral (strategic) elements, which seems to match the direction being taken by the EU Commission for their 'strategic thinking' on INCO for Horizon 2020 [19]. However, as these new proposed longer term structures are beyond the original scope of the BIC IAG and WGs, focus in the next year (2013) should include mechanisms for continuing and advancing this work after BIC concludes at the end of 2013.

Finally, for the next year of BIC, the IAG workshop concluded the following should be addressed with more emphasis and vigour:

- Cyber crime and forensics;
- Cyber hacktivism (malicious rumours);
- Multi-lateral approaches towards Cyber Security research as being advocated in BIC;
- Use of "Mobile" and "Cloud" as a driver for international cooperation in emerging countries.
- Security as a service;
- Trust models in different cultures (westernised and collectivised) – how to jointly learn from these experiences;
- Further elaboration of "Success Metrics" for INCO at a programme level;
- Further scoping of the IAG/WGs structure for multi-lateral INCO.
- Identifying mechanism(s) for the continuing and advancement of building long term multi-lateral structures initiated in BIC to carry forward the ideas into Horizon 2020.

8. Further information

8.1 References

[1] Euro-Africa ICT project http://euroafrica-ict.org/

[2] BIC website http://www.bic-trust.eu

[3] BIC Annual Forum 2012 website http://www.bic-trust.eu/events/bic-forum-2012/

[4] BIC Working Groups Workshop report http://www.bic-trust.eu/events/bic-workshop-on-the-cross-domain-coordination-of-international-cooperation-day-1-and-technical-themes-in-trustworthy-ict-and-inco-day-2/

[5] BIC Deliverable D2.3 - Interim report of the Working groups activities (restricted).

[6] DIT, Cyber laws strategy, http://www.mit.gov.in/content/cyber-laws

[7] DIT, Cyber Security R&D strategy, http://www.mit.gov.in/content/cyber-security-r-d

[8] DIT, Organisation chart 2/5, http://www.mit.gov.in/content/organization-chart

[9] http://cordis.europa.eu/fp7/ict/security/home_en.html

[10] DIT, Cyber Appellate Tribunal (CAT), http://www.mit.gov.in/content/crat-dpl-other

[11] DIT, Indian Computer Emergency Response Team (ICERT), http://www.mit.gov.in/content/icert-dpl-other

[12] DIT, Controller Of Certifying Authorities (CCA), http://www.mit.gov.in/content/cca-dpl-other

[13] Information Technology Act, 2000, http://cca.gov.in/rw/pages/informationtechnologyact2000.en.do

[14] Certifying Authorities, http://cca.gov.in/rw/pages/becoming_ca.en.do

[15] Department of International Cooperation & Industrial Promotion, Bilateral Trade Division, http://www.mit.gov.in/content/europe

[16] DIT, Cyber Security R & D Call for proposals http://www.mit.gov.in/sites/upload_files/dit/files/CyberSecurity.pdf

[17] ENISA report on the Monetization of Privacy Fe. 2012: Online: http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/monetising-privacy

[18] Euro-Africa ICT 2012 Forum. Event report http://euroafrica-ict.org/files/2012/12/EuroAfrica-ICT_P8_Forum_Event_report.pdf

[19] Oliveira, Carlos, BIC Annual Forum presentation, 27th Nov. 2012, Online: http://www.bic-trust.eu/files/2012/10/OLIVEIRA_BIC27Nov2012.pdf

8.2 Link to the Workshop Webpage, where all slides can be found.

http://www.bic-trust.eu/events/bic-forum-2012/

8.3 Reminder list of upcoming events

A BIC technical workshop will be held in Q2/Q3 2013 and the BIC Annual Forum 2013 will be held again in Q4 2013.

8.4 Registered Attendees

Name**	Organisation	Country
Dereje Yohannes ASHENAFI	Adama Science & Tech. University	Ethiopia
Karima BOUDAOUD	I3S Laboratory - University of Nice Sophia Antipolis/CNRS	France
Jean CARLO ROSSA HAUCK	GQS	Portugal
James CLARKE	Waterford Institute of Technology - TSSG	Ireland
Manmohan CHATURVEDI	Pri Cons, RTD, Beyond Evolution & Researcher at IIT Delhi	India
Marijke COETZEE	University of Johannesburg	South Africa
Daan DU TOIT	Department of Science and Technology, Gov't South Africa	South Africa
Jan ELOFF	SAP Research / Meraka UTD, University of Pretoria	South Africa
Carmen FERNANDEZ-GAGO	University of Malaga	Spain
Gerardo FERNANDEZ-NAVARRETE	NICS Lab - University of Malaga	Spain
Nils JENSEN	Stockholm University and KTH	Sweden
Mounib MEKHILEF	Ability Europe Ltd.	France
Michael KAMUTI KATUNDU	Communications Commission of Kenya	Kenya
Eunice KARIUKI	Kenya ICT Board (KICTB)	Kenya
A.S.A KRISHNAN	DIT, Government of India	India
George MULAMULA	Tanzania Commission for Science and Technology	Tanzania
Patrick MUSSA	University of Malawi (UNIMA)	Malawi
Miguel NETO	Universidade Nova de Lisboa	Portugal
Carlos OLIVEIRA	European Commission	Belgium
Aljosa PASIC	Atos Spain	Spain
Michel RIGUIDEL	Telecom ParisTech	France
Mohamadou Arabani SAIBOU	l'Ecole Supérieure Multinationale des Télécommunications (ESMT)	Sénégal
Abhishek SHARMA	Beyond Evolution Tech Solution Pvt. Ltd.	India
Priscila Solis BARRETO	University of Brasilia	Brazil
Neeraj SURI	TU Darmstadt	Germany
Barend TAUTE	Council for Scientific and Industrial Research Meraka Institute	South Africa
Camille TORRENTI	Sigma Orionis	France
Karine VALIN	Sigma Orionis	France
Artsiom YAUTISUKHIN	National Research Council of Italy	Italy

** Note: if your name is missing, please let jclarke@tssg.org know

8.1 Final Agenda and terms of reference

Terms of reference (morning)

a. Identification of country wise projects and research priorities for international cooperation;
b. Identification of tangible project/programme mechanisms;
c. Identification of success metrics for international cooperation;
d. Establishment of the BIC/ IAG structure with long term strategic perspectives including modalities of other functional and special interest groups;
e. Identification of Work Items for BIC Working Groups.

Agenda

Time	Description	Speakers
10:00 – 10:20	Overview / Purpose of Meeting BIC / IAG status	Jim Clarke, Waterford Institute of Technology -TSSG
10:20 – 10:50	BIC Working Group updates	WG1. Aljosa Pasic WG2. Michel Riguidel WG3. Jim Clarke
10:50 – 11:15	Discussions about the WGs Determining a comprehensive coverage of topics required; any gaps? Identifying key topics for workshops in 2013	All contributing
11:15 – 11:30	Coffee break	
11:30 – 12:30	Interventions on hot topics of interest per country for international cooperation	Some suggestions for speakers: Jan Eloff (SA), MM Chaturvedi (India), Priscila Solis-Barreto (Brazil), Artsiom Yautsiukhin, National Research Council - C.N.R., Italy; Mounib Mekhilef, Ability Europe Ltd., France Others welcome to contribute.
12:30 – 13:00	BIC long term strategy and approach for INCO	Joint presentation of Jim Clarke and Abhishek Sharma
13:00 – 13:30 (we can extend to 13:45 also)	Discussion on the hot topics presented. Invite interventions / responses / suggestions / advice from everyone Is this the way to move forward? Final planning for afternoon panel session.	All contributing

Terms of reference (afternoon)

a. Country by country view on approaches for international cooperation;

b. Examination of trust management models in different contexts and cultures and determining the mutual benefit for international cooperation;

c. Analysing differences, commonalities, synergies between the trust models based in the western world and emerging countries with a view to collaboration;

d. Discussion of the impact on various technologies including mobile and cloud infrastructures in order to support and grow business ecosystems.

e. Identification of on-going projects and the building of tangible project ideas forming;

f. Next steps – way to move forward on this topic.

Time	Description	Speakers
13:45 – 14:45	Lunch	
14:45 – 15:00	Overview / Purpose of Workshop	Jim Clarke, Waterford Institute of Technology -TSSG
15:00 – 16:30	Programme Management session	
	South Africa	Daan du Toit, Minister Counsellor (Science and Technology): South African Mission to the European Union
	Brazil	Priscila Solis-Barreto, on behalf of CTIC and CNpQ
	India	Abhishek Sharma, BIC IAG member, obo A.S.A Krishnan, Sr. Director, Dept of Electronics & Information Technology Government of India
	Europe	Carlos Oliveira, DG CONNECT-F3 Programme Coordination, European Commission
	Management Structure for Multilateral INCO & Summary of IAG meeting	Abhishek Sharma, BIC IAG member, Beyond Evolution Tech Solutions, New Delhi, India
16:30 – 16:45	Break	
16:45 – 18:00	Panel session on trust management models approaches across countries	**Panelists**
	South Africa	Jan Eloff, SAP Research Marijke Coetzee, Univ of Johannesburg Barend Taute, CSIR
	Brazil	Priscila Solis-Barreto, University of Brasilia
	India	MM Chaturvedi, Beyond Evolution & IIT Delhi Abhishek Sharma, Beyond Evolution Tech Solutions, New Delhi
	Europe	Artsiom Yautsiukhin, National Research Council - C.N.R., Italy Karima Boudaoud , Centre National de Recherche Scientifique, France, Mounib Mekhilef, Ability Europe Ltd., France
18:00 – 18:30	Closing session & next steps	All contributing

For more details, please visit the BIC IAG Workshop site at http://www.bic-trust.eu/events/bic-forum-2012/

A1. Annex 1. Position papers and presentation summaries

A number of position papers for the BIC IAG Annual Forum 2012 were solicited on topics for international cooperation. These include the following:

Author	Organisation	Topic name	Country
Abhishek Sharma	Beyond Evolution Tech Solution Pvt Ltd	Strategy: Ways to Move Forward on INCO & Energise Collaborative Research	India
Barend J E Taute,	CSIR Meraka Institute, Pretoria	Timely cybercrime information sharing between ISPs/Telcos and banks/police	South Africa
Marijke Coetzee	University of Johannesburg	Trust models addressing cultural differences between communities	South Africa
Aljosa Pasic	AtoS	Data sharing tools for cyber security	Spain
MM Chaturvedi	Beyond Evolutions Tech Solutions & IIT Delhi	Research on “Online Trust” construct in Indian context	India
James Clarke	Waterford Institute of Technology,	Trust and Security of the Internet of Things	Ireland
MM Chaturvedi	Beyond Evolutions Tech Solutions & IIT Delhi	Privacy & Security of Mobile Cloud Computing (MCC)	India
Michel Riguidel	Telecom ParisTech	Worldwide usage control of digital data and computer programs	France
Karima Boudaoud	I3S Laboratory - University of Nice Sophia Antipolis/CNRS, France	International cooperation for Trust Management	France
Carlos Oliveira	European Commission, DG CONNECT, Communications, Networks, Content and Technology, Programme Coordination Unit (CNECT F3)	EU research and innovation in ICT - an international cooperation perspective	Belgium

A1.1 Strategy: Ways to Move Forward on INCO & Energise Collaborative Research

Author: Abhishek Sharma, Beyond Evolution Tech Solution Pvt Ltd.

Abhishek Sharma is founder, MD & CEO of Beyond Evolution Tech Solutions Pvt Ltd(beTS). Abhishek has built beTS from scratch developing many mobile application and Solutions offering niche Utility VAS as ASP to large mobile users through many large Telcos like Vodafone, BSNL, MTNL, Idea, Airtel etc in India and abroad. Prior to founding beTS, Abhishek has worked for Indian Air Force for about 22 yrs and then for large corporate in India and abroad such as Programme Manager, GSM Backhaul/ Microwave Services, Tata Telecom, India; Country Head – Telecom SBU at TCS/ Tata Infotech, India; MD at Globacom Cellular, Nigeria etc where he managed large ICT Projects & Operations such as Radar, Telecom NW, BSS, OSS etc. Abhishek is also a renowned consultant on Mobile VAS, Telecom Network, Radar Data Systems & Avionics. Abhishek is B.E. in Electronics & Telecommunications, M.Tech Computer Sc (IISc) & M.B.A. in Marketing.

1. ***Description of topic that requires INCO:***

a. Strategy to move forward on international cooperation on Projects for collaborative research.

b. Identification of need for a system to transform the current bi-lateral and overlapping country to country cooperation into a comprehensive and coordinated multilateral global cooperation.

c. Identification of various key elements that are essential to be considered to define the objectives and manage the project, duly taking into consideration the challenges associated with a multi-disciplinary, multi-lateral approach towards international cooperation for projects of Global dimension and Cross-Domain activities.

d. Deciding on the management structure with clear scope of work (SOW), hierarchy and role and responsibilities at each level to imbibe INCO on projects of global interests and ensure successful culmination of such projects viz a viz the defined tangible/ intangible deliverables of each.

e. Approach for effective deployment, dissemination and utilisation of the projects for by the societies of different countries under INCO.

2. The stakeholders involved.

The topic has three main stakeholders:

a. Researchers: These are the specialists of the field who are expected to explore various options, carry out necessary research and design the proposed solutions.

b. Govt. Bodies related to the area of research are required to examine and evaluate the proposals, allocate the funds, formulate the process of regulating the required funds and disburse the same in accordance with the defined process.

c. Industry: Role of the industry shall be to develop the products and solutions based on the designs provided by the researchers and take the developed products/ solutions to the market, to the people.

3. Benefits, Success Metrics and need for INCO on topic

a. *Benefits: The benefits of proposed strategy derived based on INCO are:*

i. Consolidation of numerous projects across the globe, their systematic prioritisation and rational distribution amongst different research bodies across the member countries.

ii. Building healthy collaborative INCO environment, acceptance of right usability projects, leveraging on mutual strengths, avoiding duplicity and identification of definite and discrete deliverables.

iii. Structured and time bound management of project and resources, effective utilisation of funds and other resources, defined way forward for planned and systematic industrial development, dissemination and people utilisation of projects.

b. *Success Metrics:*

i. Availability of consolidated and scrutinised list of Research Projects amongst member countries.

ii. Increased number of collaborative projects in progress.

iii. Achievement of Project Milestones as per plan.

iv. Improved and more cost effective utilisation of funds.

v. Clear roadmap for future expansion and smooth roll out of BIC 2013 into H 2020.

c. *Need for INCO:* A lot of research work on "Trust & Security" is going on across different parts of the world independently involving many individuals and research organizations. Unfortunately most of it is happening in isolation with no structured system for coordination and collaboration amongst each other. The only access of each others' work is through methods of published papers, journals etc. Therefore, there is strong need to create a platform and associated mechanism which can bring all such work together in such a fashion that there is systematic and regular information exchange and mutual support. This cooperation platform would facilitates the work to become well coordinated and consolidated such that their consolidated work is very comprehensive and easily usable by member countries without ambiguity or duplicity.

4. ***Approach - Bi-lateral, multi-lateral or combination of both:*** In the diverse environment of global research, while a multi lateral ICO approach may sound most appropriate, there are scenarios where topics of research may be interest only to specific countries or regions and hence it may not be prudent to totally dispense with bi-lateral approach. However while this regional approach may work for higher level themes, it may not be suitable when a particular research topic, e.g. cyber security, which needs to be addressed multi-laterally and the bi-lateral approach shall not be suited for this type of longer term strategic activity. The other aspects of the approach are:

a. Inclusive & all pervasive approach is essential to build up the right team and the scope of the project.

b. Management Structure commensurate with the SOW and deliverables.

c. Long Term Strategy for *Inclusion of Future Projects*.

d. Structured Multi Lateral Approach: Should have three main layers with specific role.

   i. Core Working Group(CWG) ;

   ii. Extended Working Groups(EWGs) - specific for each participating country and

   iii. Special Function Groups – To be under EWGs as specialists at functional level.

5. ***Timeline / Roadmap:*** A well defined Vision, Mission & Targets is essential. While the objectives should have a vision beyond an estimated period of time say five years, there has to be mission oriented approach for achievements in medium length of time, say 3-5 years. At the same time the progress of the project must also define short term action plans and targets that must be achieved within the time blocks of 3 months, 6 months and one year.

A1.2 Timely cybercrime information sharing between ISPs/Telcos and banks/police

Author: Dr Barend J E Taute, Manager: ICT Contract R&D at the CSIR Meraka Institute, Pretoria, South Africa

Barend Taute is an electrical engineer with a PhD in Electromagnetics from the Ohio State University, Ohio, USA. He has been with the CSIR since 1983, involved in research, development, technology management and business development in areas such as radar, antenna design, microwave heating, remote sensing, safety & security technologies, crime prevention, information security and ICT. Taute is the South African National Contact Point for promoting participation in the European Framework Programme 7, Security Theme, and as such a partner in FP7 project SEREN2 (Network of Security NCPs). In addition, he is a partner in the FP7 project EuroAfrica-P8 that promotes ICT dialogues, networking and analysis of research priorities between Europe and Africa. He collaborates with the South African Department of Science and Technology on ICT related bilateral relationships in Africa and Europe and is a member of the E-Commerce Advisory Committee in South Africa.

1. *Description of topic that requires INCO:*

- the background/definition of the topic;
- research challenges involved with the topic that require INCO;
- objectives of the topic that require INCO;
- the expected outcomes of dealing with that topic.

The global experience is that cyber crime (theft of money, private details or Intellectual Property, malicious attacks, fraud, money laundering, 419 scams, cyber bullying etc) are becoming more prevalent and more sophisticated – requiring police, banks and other agencies to act fast, often in real time, in order to reduce loss of money, collect evidence and identify perpetrators. Most of the data and activities happen in cyberspace and can easily cross international borders.

Key challenges for investigators include the need for **quick** identification of the source (IP address, device number, physical location, person) and to gather evidence (SIM swaps, logon details, etc) that can stand up in court or be used to block criminal activity. Criminals can quickly erase their tracks or set up alternative channels / servers / identities.

A lot of the information required for criminal investigations reside with the ISPs and Telcos, but sharing this is limited by legislation that includes issues of privacy and freedom of speech.

Research Objective: To develop a legal / technical framework for timely / real-time information sharing between Telcos / ISPs and banks / police to enable reactive and proactive cybercrime investigations. This would study the optimal set of technical data requirements as well as various national and international legal regimes in order to arrive at a useful set of data requirements, means to access them and legal authority to do so.

Expected Outcome: A Framework for Timely Data Sharing to Support Criminal Investigations that takes a global view of the data needs of cybercrime investigators and seeks to define an optimal legal basis that will allow ISPs and Telcos to provide such information. This could then be used to advise international and national legal modernisation initiatives.

2. Who are the stakeholders involved (and how best to mobilise them)?

- Cybercrime investigators: Police and Financial Institutions. They have the challenge to investigate and stop criminal activity. International agencies like InterPol and national/international banking associations could verify the needs and support a project.
- ISPs and Telcos that have access to data that can support investigations. Various national / international associations. They typically need to protect privacy, reputation and revenues and would need a sound and safe solution.
- National and international legal academics, legislators and regulators such as the International Telecommunications Union. This is probably already on their agenda and needs to be explored with them.

3. State the benefits, and success metrics and need for INCO on topic:

Benefits: Parallel studies in a variety of countries / continents will highlight the spectrum of crime types, legal challenges, technical issues and possibly creative solutions that have already been found.

Success metrics: A Framework that can be adopted internationally and that will guide national legislative modernisation.

4. Approach: What is approach to take: bi-lateral (country to country); multi-lateral (multiple countries); combination of both, and why?

Telcos/ISPs operate nationally and globally and criminal activities know no boundaries. A multi-national approach from the beginning will enhance the benefit for the global community.

5. *Timeline / roadmapping (what needs to be done and when it should be done):*

- Q1: Verification of problem statement
    - Interaction with national Legislators / Financial Institutions / Police in a number of targeted countries to refine the problem statement and requirements for investigators.
    - Contact with international legislators, agencies and regulators to identify current initiatives and to verify the legal limitations / processes.
    - Mobilisation of stakeholders to support the project's objectives
- Q2, Q3: Analysis
    - Multi-pronged approach to gather detailed national and international information
- Q4: Design
    - Development of a framework
- Q5: Validation
    - Testing the framework with all stakeholders, updating and refinement
- Q6: Promotion and implementation
    - Seeking support from stakeholders that can influence implementation.

A1.3 Trust models addressing cultural differences between communities

Author: Marijke Coetzee, Academy for Computer Science and Software Engineering at the University of Johannesburg, South Africa

Marijke Coetzee is a Professor in the Academy for Computer Science and Software Engineering at the University of Johannesburg, where she is also the sub-head of Computer Science. The main focus of her research focus is on Information Security, specifically security policy specification and evaluation, information security of service-oriented architectures and mobile and wireless environments, and trust for mobile social network applications. She is a rated NRF researcher and has co-authored 40 papers published in peer-reviewed local and international conference proceedings and journals. She acts as reviewer for various national and international conferences, is the external moderator of a number of post-graduate subjects at other tertiary institutions, and a co-chair of the ISSA (Information Security for South Africa) conference. She is a member of the ACM, IEEE and SAICSIT.

1. *Description of topic that requires INCO:* 2-3 paragraphs highlighting:

A research topic for identified for international cooperation is the development of trust models, mechanisms and architectures to support business ecosystems in rural Africa. For these systems, it is important that trust management takes into account concepts relevant to the target context. An important identified focus of the research is the study of culture on trust. Cultural differences, while difficult to observe and measure, are obviously very important. Failure to appreciate and support them can lead to embarrassing blunders, and lower economic activity and performance.

For *Individualistic* cultures, for which most trust management systems have been developed, consumer trust is facilitated through trust mechanisms such as institutional guarantees, laws and policies, information security mechanisms, and social controls. In contrast, *Collectivist* cultures, found in Africa, Asia, India and South America have different needs as they interact in different ways. For example, in collectivist cultures people emphasize interpersonal relationships where loyalty is obtained by protecting the group members for life. Individuals see themselves as subordinate to a social collective such as a state, a nation, a race, or a social class. They prefer group harmony and consensus to individual achievement.

The research challenges entail:

- A study of existing cultural frameworks to determine the most suitable to use;
- Extraction of relevant cultural behaviours and beliefs that are applicable to consumer trust;
- A study of trust models to identify the most applicable to use for business ecosystems in rural Africa;
- The enhancement of trust models with cultural norms;
- The implementation and evaluation of a prototype system to determine if the culturally adapted trust model can be used in rural communities.

The objectives of the topic that require INCO:

The objectives are to identify the role of culture in consumer trust. This research objective is of interest not only to the African context, but to any environment where different types of cultures exist, and where an understanding of the influence of culture on trust is limited. It is therefore a topic that is ideal for collaboration between parties found in different countries in Europe, Africa, India and Brazil.

The expected outcomes of dealing with that topic.

A framework that gives support on how to adapt trust models to culture.

2. Who are the stakeholders involved (and how best to mobillise them)?

Currently:

South Africa:

University of Johannesburg and SAP research Pretoria, South Africa

Possible partners have been identified already from India and the EU but more are welcomed to mobilise in a bid for funding of a joint project to investigate the manner in which each partner country can benefit from this research.

3. State the benefits, and success metrics and need for INCO on topic:

The project will bring more understanding of the role of culture on consumer trust.

Success metrics:

A working prototype, evaluated in a real life context.

Need for INCO:

- Funding to do more investigation on cultural behaviours and norms and consumer trust in different contexts.
- Assistance with the evaluation of the prototype in a real community such as India.

4. Approach: What is approach to take: bi-lateral (country to country); multi-lateral (multiple countries); combination of both, and why?

Both approaches are needed because different countries have different perspectives on this problems, which needs to be accommodated.

5. *Timeline / roadmapping (what needs to be done and when it should be done):*

very provisional..

- Investigation of culture on consumer trust – on-going till 2015
- Completion of basic model developed in South Africa - by end of 2013
- Evaluation of prototype - start of 2014 - 2015
- Continuous adaptation of trust model based on prototype evaluation - 2014 – 2015.

A1.4 Data sharing tools for cyber security

Author: Aljosa Pasic, Atos, Spain

ALJOSA PASIC current position is Business Development Director in Atos Research & Innovation (ARI), based in Madrid, Spain. He graduated Information Technology at Electro technical Faculty of Technical University Eindhoven, The Netherlands, and has been working for Cap Gemini (Utrecht, The Netherlands) until the end of 1998. In 1999 he moved to Sema Group (now part of Atos) where he occupied different managerial positions. During this period he was participating in more than 50 international research, innovation or consulting projects, mainly related to the areas of information security or e-government. His current interests include Secure Software Engineering (as the chairman of NESSOS industry advisory group), electronic identity and privacy, GRC (governance, risk and compliance) as well as cyber security. He is member of EOS (European Organisation for Security) Board of Directors, and collaborates regularly with organisations such as ENISA, IFIP, IARIA, FI-PPP and others.

1. *Description of topic that requires INCO:* 2-3 paragraphs highlighting:

The recent attack clearly showed how cyber security data sharing tools, policies, and infrastructures failed in front of a global threat that was designed to focus against a specific user target, but it affected many countries.

The main constraint and challenge for international cyber security research is the lack of trust that needs to be evaluated, analyzed, used, negotiated. INCO is needed in research on trust model and their link to cyber security infrastructures and strategies, and outputs could range from data sharing schemes based on e.g. incremental sharing to specific mechanisms to process cyber security data.

2. Who are the stakeholders involved (and how best to mobillise them)?

Research and industry from various countries, critical infrastructure operators , CERT and CSIRT teams etc.

3. State the benefits, and success metrics and need for INCO on topic:

Improved situational awareness and cyber security incident management.

4. *Approach: What is approach to take: bi-lateral (country to country); multi-lateral (multiple countries); combination of both, and why?*

Multi-lateral since the threat propagation is not predictable.

5. *Timeline / roadmapping (what needs to be done and when it should be done):*

ASAP

A1.5 Research on "Online Trust" construct in Indian context

Author: MM Chaturvedi, Principal Advisor Research & Technology Development, Beyond Evolution Tech Solutions Pvt. Ltd., India

Air Cmde MM Chaturvedi is a retired Indian Air Force officer. His PhD thesis in Information Security area is under review at IIT Delhi. He has about 35 years of experience in managing technology for IAF. An alumnus of National Defense College, New Delhi, he has held various appointments dealing with telecommunication policy issues. He graduated from Delhi College of Engineering and completed post graduation from IIT Delhi. Current interests include vulnerability analysis of evolving ICT infrastructure. Currently he is a visiting faculty at IIT Delhi and Ansal University Gurgaon, besides consultant at Beyond Evolution Tech Solutions Pvt. Ltd., India.

1. Description of topic that requires INCO:

- The potential uptake of the mobile computing in tandem with cloud paradigm offers possibilities that can spur a huge market in developing Indian economy
- However, the privacy and security concerns because of the necessity to store data at remote locations seem to be an inhibitor for both corporations and individuals

2. Research challenges involved with the topic that require INCO:

- Trust in the clouds is currently characterized by conflict between earlier approaches to data protection requiring its storage in private locations and the current technology that protects and uses data by spreading it across remote geographically dispersed public domains
- While the current approach is considered technologically superior and safer as bank lockers are statistically safer compared to home vaults; the user mindset is slow to change and we need to package these innovations with an eye on the underlying reluctance of the potential consumer.

3. Who are the stakeholders involved (and how best to mobilise them)?

Evolving Indian Government Policy

- The Central Government, the State Government and public authorities shall deliver all public services by electronic mode within five years of the commencement of this Act (**THE ELECTRONIC DELIVERY OF SERVICES BILL by Indian Government, 16th November 2011)**
- In an endeavor to increase citizen's trust in the online environment and to enable the various government agencies to choose appropriate authentication mechanisms, the Department of Information Technology, Government of India has conceptualized the National e-Authentication Framework (NeAF) **(Draft National e-Authentication Framework (NeAF) by Indian Government, 01 Sep 2011)**
- The m-Governance framework of Government of India aims to utilize the massive reach of mobile phones and harness the potential of mobile applications to enable easy and round-the-clock access to public services, especially in the rural areas. The framework aims to create unique infrastructure as well as application development ecosystem for

m-Governance in the country **(Framework for Mobile Governance by Indian Government, Jan 2012)**

4. State the benefits, and success metrics and need for INCO on topic:

- The above listed policy initiatives by Indian Government provide the context for this research
- The **National e-Authentication Framework (NeAF)** is borne of the compulsions to ensure secure online delivery of e-governance services across various platforms including mobile.
- Mobile governance framework has emphasized the need for leveraging the high penetration of mobile platform to facilitate citizen engagement
- The proposed research aims to analyse these frameworks in depth through the lens of "**Online Trust**" construct
- Our success in engaging citizen would depend in understanding the deep drivers of their trust towards offered services
- Following tangible gains may be achieved by the proposed research:
  - *Taxonomy of privacy and security technology*
  - *Inputs for policy on mobile cloud computing*
  - *A trust model and guidelines for implementation*
  - *Knowledge dissemination*

5. Approach: What is approach to take: bi-lateral (country to country); multi-lateral (multiple countries); combination of both, and why?

- The psychology of trust has deeper connotations and is influenced by the cultural backdrop of the people being investigated
- For ensuring adequate uptake for the mobile cloud applications we need to package them with due sensitivity to the trust dynamics of the target consumers
- There is a case to undertake a research in the construct of "Online trust" models as applicable to the adoption of these emerging mobile applications in Indian and International context. The common denominators and differences amongst the researched cultures would provide deep insights while designing security and privacy applications.
- We need to address this challenge by engaging all stakeholders. A combination of bilateral and multilateral approach may emerge as we traverse the research path.

6. *Timeline / road mapping (what needs to be done and when it should be done):*

The research may be undertaken in phases. The research plan and deliverables at end of each phase would need preliminary study by the collaborating agencies. A time line of 3 years for useful deliverables is considered realistic.

A1.6 Topic: Trust and security of the Internet of Things (IoT)

Author: James Clarke, Waterford Institute of Technology, Ireland.

James Clarke has been working for the Waterford Institute of Technology (WIT) in the Telecommunications Software and Systems Group (TSSG), since February 2005. Prior to joining WIT-TSSG, Mr. Clarke worked at LAKE Communications in Ireland for eight years and Grumman Corporation in the United States for eight years. Since January 2011, Mr. Clarke has been the project coordinator of a European Framework Program 7 Co-ordination action entitled 'BIC[3]', which stands for Building International Cooperation for Trustworthy ICT: Security, Privacy and Trust in Global Networks & Services. Previous to this, Mr. Clarke coordinated the successful FP7 INCO-Trust [4] project. More information can be found at http://www.tssg.org/about/people/james-clarke/.

1. *Description of topic that requires INCO:*

There is still considerable RTD required by international communities for the trust, privacy and security research challenges arising from the constitution of the IoT architectures, infrastructures, communications, devices, objects, applications and services. In this short report, we present an overview of how to go about addressing this in future RTD work, specifically in Europe and beyond, regarding trust, privacy and security of the Internet of Things with a view towards enabling international cooperation efforts around the globe to solve these major research challenges. More details can be found in the SecurIT 2012 paper at [1].

There are a number of widely used definitions for Internet of Things, including the following:

"Things having identities and virtual personalities operating in smart spaces using intelligent interfaces to connect and communicate within social, environmental, and user contexts. Interconnected objects having an active role in what might be called the Future Internet." source: Internet of Things in 2020 - Roadmap for the Future. May 2008 [2]

"Objects will sometimes have their own Internet Protocol addresses, be embedded in complex systems and use sensors to obtain information from their environment and/or use actuators to interact with it". source: Internet of Things – An action plan for Europe. June 2009 [3]

"A dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols - Physical and virtual "things" have identities, physical attributes, and virtual personalities and use intelligent interfaces, and are seamlessly integrated into the information network." source: Internet of Things – Strategic Research Roadmap. September 2009 [4]

[3] http://www.bic-trust.eu/

[4] http://www.inco-trust.eu/

However, all IoT definitions revolve around the same central concept: “a world-wide network of interconnected objects” with the following attributes: existence, sense of 'self', connectivity, interactivity, dynamicity, and sense of environmental awareness.

2. The Stakeholders involved.

In order to identify the stakeholders, it is necessary to identify the research challenges that need to be addressed. As shown in Figure 1, there are a number of top level security research challenges. In summary, the challenges are the following:

Figure 2. Security research challenges in IoT

1. **Protocol and network security** to deal with the large number of objects with significant heterogeneity. This would involve improved cryptography to make them operate in smaller environments requiring faster operation while keeping same levels of security so far. A Key management infrastructure is needed for the open configuration of IoT, in which the new systems need to be able to manage the keys in objects of small size where the current certificate based systems wouldn't work. The current Internet protocols are not usable in these environments.
2. **Data and Privacy** as carrying multitudes of objects can bring up a lot of privacy issues as they are not operating in an isolated way. This area can be addressed by using Privacy by Design (user should be able to decide which of his/her information and how it is being used); Privacy by Default (right to be forgotten); transparency (he should know when it is being used), and improved data and information management.
3. **Identity management**, which must be taken from a different perspective in IoT in which objects will have a core identity and yet a temporary identity must be possible. ID management systems should encompass Identification (how to define the identity of a "Thing"); Authentication (infrastructure that allows mutual authentication based on Centralized, Distributed, Local, Global, Attributes); and Authorization based on delegation (e.g. stethoscope) and granularity (e.g. classroom provides class schedule to everyone, syllabus only provided to students).
4. **Trust and governance** is required in order to obtain trust between the different objects (and from the user perspective). For the IoT, a trust management system is especially required inside in order to gain trust management from the user perspective. From the

system perspective, governance is very important where policies should be contained and where the policies vs. control is dealt with;

5. **Fault tolerance** as the perimeters of the networks do not exist any more in IoT. Therefore, attackers will be all around and there is a need to provide solutions with the following attributes - Secure by default (Patch Tuesday?), Internal State and the ability to provide self - defence recovery.
6. Also shown in figure 1 are two special **"foundational challenges",** including those related that are **Properties / Application-specific**. These are basic properties that all challenges must consider (e.g. Interoperability, Scalability, Resilience) and to the high-level, application-specific security mechanisms that make use of all the challenges above (e.g. Secure discovery of services); and **Architecture**. Within a system, it is necessary to provide some architectural support to integrate the different security services.

3. Benefits, Success Metrics and need for INCO on topic

Benefits: The benefits of proposed strategy derived based on INCO are:

i. The research and technological development of IoT capabilities that will work in a trustworthy and secure manner across borders.

Success metrics:

ii. Achieving considerable impact from international partners in realising IoT technologies.

iii. Increased number of collaborative projects in progress.

iv. Sharing of resources and capabilities in the required areas.

v. Taking into account cultural aspects of different users of IoT technologies and systems.

Need for INCO: IoT research and technological developments are taking place at different levels around the globe and it would be more efficient and effective to pool these resources together.

4. *Approach - Bi-lateral, multi-lateral or combination of both:*

The authors would suggest to start with bi-lateral with countries very much engaged in these research areas and move to a more multi-lateral approach when the levels of research cooperation begins to grow exponentially. This suggestion is made from a more practical perspective as the building of international cooperation is difficult when using a bi-lateral approach as it takes significant time for all of the parties to come together to try to align their activities and priorities. Therefore, it is even more difficult for a multi-lateral approach when building a longer term strategy in as complex an area with so many research challenges as proposed within this short paper.

5. *Timeline/roadmap:*

Within figure 2, the challenges are configured into a timeline as introduced by *Internet of Things: Strategic Research Roadmap* [5] and the *Towards a Trustworthy Information Society Think-Trust report* [6]. As seen in the figure underneath the timeline, there are a number of research items (e.g. trust management, access control (delegation) and governance) that don't easily fit yet into the timeline and the research community needs to urgently work together closely to determine when and how these challenges should be addressed for IoT.

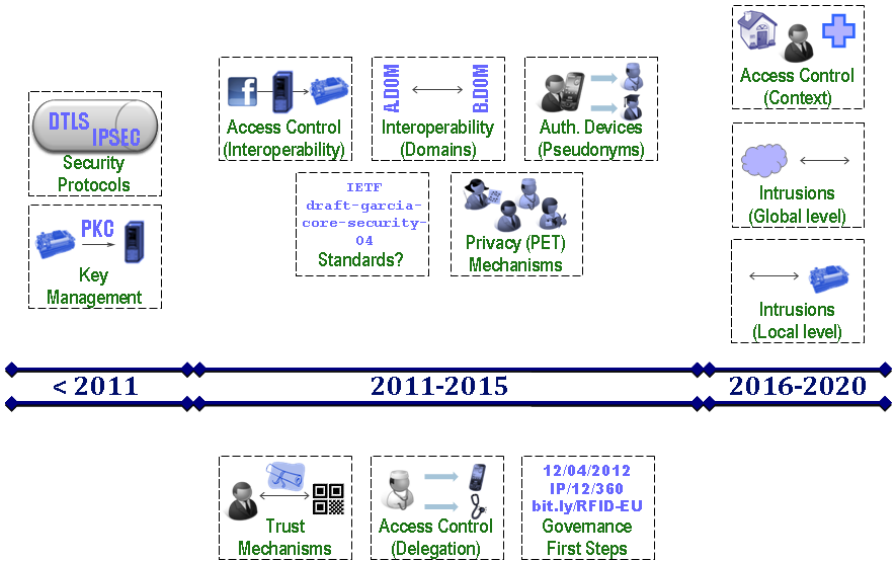

Figure 2. Research challenges in a timeline

Although a considerable amount of research has already been undertaken for IoT, there needs to be considerable more research carried out in particular with respect to trust, privacy and security elements. It should be noted that while the data here is as accurate as the authors could conclude from their research and interactions in the aforementioned events and documents, there could be existing studies already being carried out on these items not included here (e.g. in an European project, where public deliverables are sometimes limited), or there may be additional challenges not considered in detail within our analysis. Therefore, this paper is being used to draw feedbacks from the INCO research communities on these topics in which readers and listeners could certainly clarify something and to share their knowledge with the authors and other attendees. Figure 3 depicts research areas where we are lagging behind in the timeline formation.

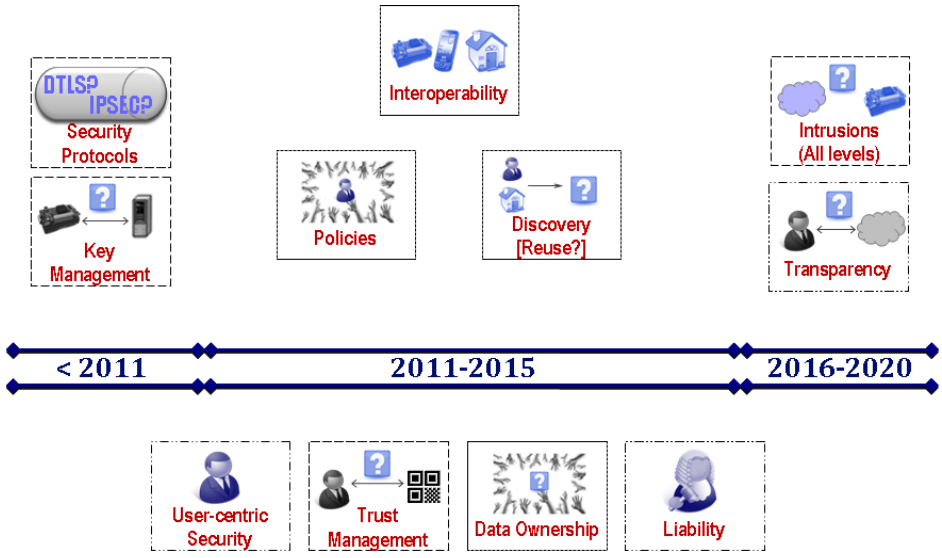

Figure 3. Future research challenges required in timeline

6. *References*

[1] Clarke, J., Suri, N., Sharma, Lopez, J., Roman Castro, R., Trust & Security RTD in the Internet of Things – Opportunities for International cooperation, SecurIT 2012, Kerala, India, 14-16th August 2012, ACM Publications.

[2] ftp://ftp.cordis.europa.eu/pub/fp7/ict/docs/enet/internet-of-things-in-2020-ec-eposs-workshop-report-2008-v3_en.pdf

[3] http://ec.europa.eu/information_society/policy/rfid/documents/commiot2009.pdf

[4] http://www.internet-of-things-research.eu/pdf/IoT_Cluster_Strategic_Research_Agenda_2009.pdf

[5] Vermesan, O., et al. 2011, Internet of Things Strategic Research Roadmap, published by The IoT European Research Cluster — European Research Cluster on the Internet of Things (IERC). http://www.internet-of-things-research.eu/pdf/IoT_Cluster_Strategic_Research_Agenda_2011.pdf

[6] Foley, B., Sullivan, K., et al., 2010. Towards a Trustworthy Information Society - Report of the RISEPTIS Advisory Group, published by the FP7 Think-Trust project. http://www.think-trust.eu/riseptis.html

A1.7 Privacy & Security of Mobile Cloud Computing (MCC)

Author: MM Chaturvedi, Principal Advisor Research & Technology Development, Beyond Evolution Tech Solutions Pvt. Ltd., India

Air Cmde MM Chaturvedi is a retired Indian Air Force officer. His PhD thesis in Information Security area is under review at IIT Delhi. He has about 35 years of experience in managing technology for IAF. An alumnus of National Defense College, New Delhi, he has held various appointments dealing with telecommunication policy issues. He graduated from Delhi College of Engineering and completed post graduation from IIT Delhi. Current interests include vulnerability analysis of evolving ICT infrastructure. Currently he is a visiting faculty at IIT Delhi and Ansal University Gurgaon, besides consultant at Beyond Evolution Tech Solutions Pvt. Ltd., India.

1. Description of topic that requires INCO:

- There is a need for a lightweight secure framework that provides security with minimum communication and processing overhead on mobile devices
- The security and privacy protection services can be achieved with the help of secure cloud application services
- In addition to security and privacy, the secure cloud application services provide the user management, key management, encryption on demand, intrusion detection, authentication, and authorization services to mobile users

2. Research challenges involved with the topic that require INCO:

- The proposed research would attempt to leverage the strengths of Mathematics and Electrical Engineering departments at IIT Delhi. As the threats to mobile devices are emerging and solutions to counter them are challenging, any collaboration with other International academic institutions on the proposed research would result in synergy of efforts.
- The Indian government has chosen mobile device as preferred platform to engage with citizens while offering various e-Governance services. Likewise there is huge market for mobile based e-Commerce applications.
- Our ability to convincingly address the security and privacy concerns of the growing Indian market using the experience and current research efforts of developed European member states can help us meet this social challenge.

3. Who are the stakeholders involved (and how best to mobilise them)?

- The collaborating research institutions in India and in developed countries would stand to gain by meeting the existing demand for secure and private transactions through a mobile device.
- At national level while boosting the economy of collaborating nation states, the security of the future mobile transaction would help us achieve the objective of a secure and safe Information Society.
- The stakeholders are being identified through personal interactions and any institutional support from European Commission would go a long way to reach the stated objectives faster.

4. State the benefits, and success metrics and need for INCO on topic:

- The collaborating research institutions in India and in developed countries would stand to gain by meeting the existing demand for secure and private transactions through a mobile device.
- At national level while boosting the economy of collaborating nation states, the security of the future mobile transaction would help us achieve the objective of a secure and safe Information Society.

5. Approach: What is approach to take: bi-lateral (country to country); multi-lateral (multiple countries); combination of both, and why?

- The challenge to secure mobile transactions from emerging threats is a multidisciplinary issue. The use of mobile devices for many sensitive transactions is growing in developed and developing economies alike.
- We need to address this challenge by engaging all stakeholders. A combination of bilateral and multilateral approach may emerge as we traverse the research path.

6. Timeline / road mapping (what needs to be done and when it should be done):

The research may be undertaken in phases. The research plan and deliverables at end of each phase would need preliminary study by the collaborating agencies. A time line of 3 years for useful deliverables is considered realistic.

A1.8 Worldwide usage control of digital data and computer programs

Speaker: Michel Riguidel, Telecom ParisTech, France

Michel Riguidel is now Professor Emeritus (since May 2010), previously the Head of the Department of Computer Science and Networks, at Telecom ParisTech (École Nationale Supérieure des Télécommunications, www.telecom-paristech.fr) in Paris, where he lectures in security and advanced networks. His research is oriented towards security of large Information Systems and Networks and architecture of communication systems (Security of the Future Internet, Trust, Privacy and Advanced Networks).

In the European Projects, he was Key Researcher of the Secoqc Project (Development of a Global Network for Secure Communication based on Quantum Cryptography). In the FET of the FP6, he was the Security & Dependability Task Group Leader of the Beyond the Horizon Project. He has actively contributed to the Coordination Action projects FP7 ThinkTrust, IncoTrust (2008-2010) and currently BIC (2011-2013).

He has several patents in security (firewall, watermarking and protecting CD ROM, illicit content downloading, security of communication).

In 2013, he is currently working on BIC and other international cooperation activities involving the security of the Future Internet, especially with JiaoTong University (Shanghai) and Huawei.

1. Description of topic that requires INCO: 2-3 paragraphs highlighting:

Background, definition of the topic

With the global development of network activity without borders, digital data and computer programs for users and businesses are increasingly under the management or direct control of third parties, mostly outside the borders of countries of the owner or his responsible: cloud computing, social networks, search engines, mobile applications, micro-blogs, distributed games, messages, etc.

Research challenges involved with the topic that require INCO

Usage control of computer entities (equipment, services, applications, data, and multimedia content) is a fundamental problem in digital security. There is no technical measure to fully resolve this issue, because the volatility of an entity is a consubstantial digital property: one can endlessly create, store, destroy, copy, modify, process and transmit data or a program. There is no technical measure to fully guarantee programs or data security, whose one is either owner or responsible and which are managed and controlled by third parties.

This is the problem of usage control (DRM, software license, distribution of multimedia content) and the problem of cloud computing security, or the issue of right to oblivion for personal data distributed on the net.

- Many personal data are managed by third parties (service providers on the network), created by third parties (mobile operator, bank), stored or handled by search engines, without authors, owners, or those responsible for this data or these programs have a real feedback on these data, or even scrutiny.
- Some personal data are created voluntarily, in a certain context by the people, but then become sensitive and out of their control (photo on mobile phones, personal data on social networks). Modification, annotation or erasure of data is almost impossible due to a massive boom on a content or media lynching. Other personal data are created without the knowledge or consent of people, and out of their control (recording of geo-location, bank records, database created by search engines).

• Most application software is now distributed on the network, with different business models (pay per use, license and subscription) without absolute secure lock.

In practice, usage control is implemented by some technical measures that have heavy vulnerabilities (DRM, hardware lock, electronic signature, etc.). Its implementation is actually complemented by organizational measures when it is confined to a specific area (eg project management), or legal action when it is confined in a single country (laws on intellectual property or on usage of computer resources).

Objectives of the topic that require INCO

The problem becomes more acute at the international level (cloud computing, DRM, multimedia download, software distribution), because States have not yet harmonized their legislation on counterfeiting, illegal use of content, on the data commodification, on intellectual property of programs and data, on compliance with the private info-sphere, on malevolent usage of data and programs.

• How to make computer usage less opaque: resources used, circulation and storage of data are made more opaque by virtualization. Virtualization brings a de-correlation between the physical and logical resources.

• How to change the relationship to the supplier, which has an increasing responsibility and to which a hard auditable security assurance is assumed. Do we have models to identify trustworthy providers over time?

In addition, threats exploit regulatory vulnerabilities: data governance is an issue of sovereignty. Finally, irreversibility of the access to digital data is a threat: message delivery without post-security from the recipient, proprietary format of clouds, data on social networks without time constraint, etc.

The research objective is to develop a legal and technical framework to provide security, trsut and privacy for data (personal data and software for individuals and/or enterprises) that takes a transnational perspective. This would take into account the set of technical requirements, the new context (cloud computing, social networks) for software editors and service providers to implement such environment.

The expected outcomes of dealing with that topic

An overall framework for sharing, exchanging data and programs would redesign the legal conditions, obligations and constraints of using software and data (multimedia content, etc.) in the new ecosystem: issues of copyrights, privacy questions, peer-to-peer exchanges, etc.

2. Who are the stakeholders involved (and how best to mobillise them)?

• Software editors that are designing services, ISPs and Telcos that have access to data. They typically need to protect intellectual property, privacy, reputation and revenues and would need an overall solution.

• National and international legal and technical academics, legislators and regulators.

3. State the benefits, and success metrics and need for INCO on topic:

The lack of protection is an obstacle to the adoption, by individuals or companies, of innovative services (public cloud computing for businesses, networked applications for individuals).

4. Approach: What is approach to take: bi-lateral (country to country); multi-lateral (multiple countries); combination of both, and why?

Software editors and software engineering academics are best suited to take initiatives. Then ITU and international software engineering associations could test the deployment of such framework. A multilateral and a continent to continent (America, Africa, Europe, Asia) approach is needed due to the different cultures for properties and privacies.

International cooperation in software security is too dispersed. Software engineering is too focused on formal methods and not on cross-disciplinary questions as security, property, authorship.

5. *Timeline / roadmapping (what needs to be done and when it should be done):*

It is necessary to conduct research at the international level, both technical and legal, to fill this gap, which is an obstacle to the development of digital services:

Research until 2015

Recommendation for Research 1 (R1) - Research on security models

- Security Policy of outsourcing services;

- Model of security, trust and privacy of data or programs controlled by worldwide third parties;

- Design and implementation of security models, trust models, privacy model on services applicable to personal data and behavioural data, recorded unbeknownst to the people.

R2 - Research on architectures and services

- Development of technical measures for the right to be forgotten (erase data after a certain period)

- Method and tools for the right to change (deletion, annotation, etc.) personal information.

- Design and deployment model of entrustment, delegation of management by a third party.

- Rules of monitoring or audit of management by a third party.

- Usage control model (a priori, a posteriori)

- Access control model, with information and / or permission of the authors or indirect control

- Security policy of outsourced data management

- Security of public cloud computing

R3 - legal framework

- Security of DRM, security model of intellectual property

- Secure communications with scrutiny on the operating post messages.

- Security model in association (information on usage of personal data)

R4 - ethical, economical dimensions

- Ethical usage of computing resources, data, programs

- Audit of the usage

Implementation 2015 - 2020

Then the validation of several instantiations of the framework could be tested at the national and continental levels.

A1.9 International cooperation for Trust management

Speaker: Karima Boudaoud, I3S Laboratory - University of Nice Sophia Antipolis/CNRS, France

Dr. Karima Boudaoud is Assistant Professor at the University of Nice Sophia Antipolis. She had obtained her PhD. degree in Computer Sciences from Ecole Polytechnique Fédérale de Lausanne (EPFL) and had received her M.Sc in Computer Sciences from the University of Versailles Saint Quentin-en Yvelines (UVSQ). She has participated in several research projects in the area of Networks and Services Security funded by the European Commission (IST-FP6 research programme), CNRS-INRIA-DGA and Fond National Suisse. She has served in several TPC and OC of several national and international (IEEE/IFIP or others) conferences and workshops (IM, WWW, ICC, NOMS, etc.). Her main research interest is Security management but a security management oriented towards the User and her previous research field was intrusion detection using multi-agent system.

Why do we need INCO for Trust?

The first obvious response to the question “Why do we need INCO for Trust” is that when talking about trust, we cannot ignore the influence of the culture on the concept of trust. This concept has not the same meaning in Europe or America and in Asia and south Africa due to the fact that in Europe and America it is and individualist culture whereas is Asia and South Africa it is a collectivist one [1]. In addition to the fact that culture has a major influence on trust, culture is not the only criteria to consider when talking about trust, but societal values, language differences have also an impact on trust. Thus, trust needs can be and are different from a culture or a country to another one.

Now, the next question is what do we need to understand and manage trust at a World Wide level? We need a more World Wide trust model using a multi-lateral and multi-cultural approach that:

1) first involve the end-users and listen to their trust needs; and

2) then translate these trust needs into parameters that makes sense to these end-users.

How to build a World Wide trust model?

Several powerful trust models [2][3][4][5][6][7] have been proposed to model trust in different contexts (wireless networks, sensors networks, etc.). These models use mathematical models that can be enough for this kind of context. However, if we use them in other contexts that involve the Human, such as social networks, they are useless, as they don’t take into account the cultural factors. A very good example is a study that has been conducted for online shopping and e-commerce where it has been proven that the trust model used by e-bay does not suit Asian users’ expectations [8][9].

On another hand, several multi-cultural models have been proposed such as MCR [10], however these models have not been designed for trust management. Thus, it is not possible to use them to model trust.

As a consequence, to build a World Wide trust model, we need to extend existing trust models and integrate multi-cultural aspects.

How INCO can help and how to best move forward?

From an international point of view, different actions are required, e.g. collaboration with:

- International security experts having a user-centric approach regarding trust, privacy and security (Brazil, India, South Africa, Canada, USA, France, etc.)
- International experts from different disciplines to take into account the differences in terms of culture, laws, etc.

- Collaboration with international standardization organisations such as W3C, ETSI, IETF, etc.

These collaborations can start through:

- Creation of multidisciplinary working groups in each targeted country (right experts from each discipline).
- Organization of international multidisciplinary workshops in targeted countries (involving wider public) As far as we know, a World Wide trust model does not exist and this is mainly due to the complexity of the problem as it implies Human and cultural factors which can only be possible by involving people and researchers more different cultures.
- This kind of model requires covering various regions in the World (India, China, South America, South Africa, etc.) to suit different cultural regions and languages. The only way to be able to do it is to provide a way to create and strengthen collaboration between trust experts from different cultures. This can be done through international cooperation and more specifically, international workshops and working groups.
- As a conclusion, using an international cooperation approach for a trust taking into account cultural differences is mandatory if we would like to design a multi-cultural trust model that can be understood and used by different cultures.

References

[1] D. Isherwood, M. Coetzee and J.H.P. Eloff, Towards Trust and Reputation for E-Commerce in Collectivist Rural Africa, International Symposium on Human Aspects of Information Security & Assurance (HAISA 2012), 6-8 June 2012 in Crete, Greece.

[2] Antonio Maña, Hristo Koshutanski, Ernesto J. Pérez, A trust negotiation based security framework for service provisioning in load-balancing clusters, Computers & Security, Volume 31, Issue 1, February 2012, Pages 4-25

[3] Azzedine Boukerche, Yonglin Ren, A trust-based security system for ubiquitous and pervasive computing environments, Computer Communications, Volume 31, Issue 18, 18 December 2008, Pages 4343-4351

[4] Fabio Martinelli, Marinella Petrocchi, A Uniform Framework for Security and Trust Modeling and Analysis with Crypto-CCS, Electronic Notes in Theoretical Computer Science, Volume 186, 14 July 2007, Pages 85-99

[5] Şerif Bahtiyar, Mehmet Ufuk Çağlayan, Extracting trust information from security system of a service, Journal of Network and Computer Applications, Volume 35, Issue 1, January 2012, Pages 480-490

[6] Aarthi Nagarajan, Vijay Varadharajan, Dynamic trust enhanced security model for trusted platform based services, Future Generation Computer Systems, Volume 27, Issue 5, May 2011, Pages 564-573

[7] Gabriele Lenzini, Mortaza S. Bargh, Bob Hulsebosch, Trust-enhanced Security in Location-based Adaptive Authentication, Electronic Notes in Theoretical Computer Science, Volume 197, Issue 2, 22 February 2008, Pages 105-119

[8] Daechun An, Sanghoon Kim, Effects of National Culture on the Development of Consumer Trust in Online Shopping, Seoul Journal of Business, Volume 14, Number 1, June 2008.

[9] Bessie Chong Why culture matters for the formation of consumer trust? A conceptual study of barriers for realizing real global exchange in Hong Kong Asia Pacific Management Review 8(2), 217-240, 2003.

[10] M. Mekhilef, Y. Page, M. Bel, M. Moessinger, Designing for Unrevealed Values, International Design Conference – Design 2012, Dubrovnick, Croatia, May 21-24, 2012.

The full presentation can be found at http://www.bic-trust.eu/files/2012/10/BOUDAOUD_BIC_WS27Nov2012.pdf

A1.10 EU research and innovation in ICT - an international cooperation perspective

Speaker: **Carlos Oliveira,** European Commission, DG CONNECT, Communications, Networks, Content and Technology, Programme Coordination Unit (CNECT F3)**.**

Introduction

The BIC IAG Annual forum 2012 in November 2012 was quite timely as the Commission unveiled a set of proposals during November for Horizon 2020, the new framework programme for research and innovation. This forms part of the set of proposals for all of the Union's spending programmes for the period 2014-20.

A brief overview of international cooperation in Horizon 2020 (H2020) was given during the BIC IAG Annual forum 2012 in Lisbon, Portugal on 27th November 2012 and this paper summarises the presentation.

Overview of Horizon 2020

The H2020 programme responds to the economic crisis investing in future jobs and growth. It is addressing peoples' concerns about their livelihoods, safety and environment and strengthening the EU's global position in research, innovation and technology.

In terms of the rationale for (What for?) and with whom? (country fiches), in H2020, the Commission is adopting a "strategic thinking" and the BIC report from the June 2012 workshop [1] was singled out as providing some useful material for this aspect. The approach would take into account the issues being raised by BIC and other INCO related projects, European ICT platforms, IPR, standards, instruments and cover key areas of the Future Internet, Cyber-security, micro and nano-electronics, sensor network, enterprise software, urban enviroments and e-mobility, trust and security. Included in this would be international cooperation with industrialised countries, BRICs, developing countries, amongst others.

INCO for ICT research and innovation in a globalised world was covered in the ISTAG report, which had a number of recommendations:

- Reinforce policy dialogue with 3rd countries developing a more articulated view of policies dealing market access, research and innovation;
- A more sophisticated view of "mutual benefits" – go beyond "reciprocity" in mutual research programmes;
- Safeguarding intellectual property rights is key but this should not result in excluding international partners from the possibility to exploit foreground IP;
- Simplifying "joint calls" and look for more agile forms of collaboration;
- Further develop collaboration with labs outside EU, in technological research as well as take-up and deployment (test-beds, pilots).

To find out more information about the transition to Horizon 2020, please visit

http:// www.ec.europa.eu/research/horizon2020

Also, visit the site on International Cooperation for lasting solutions http://ec.europa.eu/research/iscp

Current Mechanisms

As a number of the current mechanisms from FP7 are envisaged to still be available in Horizon 2020, the presentation concluded with how the European Commission's Framework programme 7 (FP7) has supported international cooperation, including those within areas related to trust and security research, in a number of different ways.

The first is a '**general opening**', where international partners are welcome to participate in all Challenges and Objectives with the following eligibility criteria:

- Minimum 3 different EU Member States or Associated Countries

- Beyond this minimum, all non-EU/non-AC countries can participate

The second is a '**targeted opening'**, where the participation of third countries is particularly encouraged. The targeted openings are explicitly mentioned in some of the Objectives (e.g. Australia, South Korea under WP2013).

The third is part of '**Horizontal Actions**' including bi-lateral coordinated calls. Some examples include the coordinated calls with Brazil and Japan (under WP2013) and international partnership building and support to dialogues (Objective 10.3 under WP2013).

A number of targeted openings in WP2013 were highlighted during the workshop including:

1. **Objective ICT-2013.1.5 Trustworthy ICT:** EU-Australia cooperation on building user trust in broadband delivered services

- Demonstrate in a real-life environment the maturity and practicality of a digital authentication framework in broadband delivered services working across several jurisdictions (organisational, governmental) with high levels of assurance.
- Funding: up to €3 million

2. **Objective ICT-2013.1.7 Future Internet Research Experimentation (FIRE)**:

- EU-South Africa cooperation on future internet experimental research and test-bed interconnection
- EU-China cooperation on future internet experimental research and IPv6
- EU-South Korea cooperation on future internet experimental research

3. **Objective ICT-2013.2.2 Robotics Use Cases and Accompanying Measures**:

- Robotics networking - help identify new users and markets and new research areas through sector-based analysis; establish a strategy towards sustainable international cooperation in robotics, focussing initially on the United States.

A number of coordinated calls available in WP2013 were highlighted.

1. **ICT-2013-10.1-EU-Japan Research and Development Cooperation**. A number of important events have taken place between the European Commission and EU research communities with Japan (MIC/NICT) over the last few years in the "Future Internet" domain. This work has led to the organisation of an EU-Japan coordinated call that is part of the research Work Programme 2013.

The topics for consideration include:

a) Optical communications

b) Wireless communications

c) Cybersecurity for improved resilience against cyber threats

d) Extending the cloud paradigm to the Internet of Things – Connected object and sensor clouds within the service perspective

e) Federation of test-beds: control, tools and experiments

f) Green and content centric networks

The funding scheme for the coordinated call with EU- Japan is Small or medium scale focused research projects (STREPs) with an indicative budget of EUR 9 million (a similar budget for the call is expected from the Japanese MIC and NICT). The timing for the call is 2 Oct – 29 Nov 2012.

The whole work programme is subject of an information day in Warsaw, Poland on 26 and 27 September 2012. See information at: http://ec.europa.eu/information_society/events/ictproposersday/2012/index_en.htm.

In addition, concerning the EU-Japan R&D activity, a dedicated page has been opened where you can submit your ideas, partner search, and take this opportunity to be part of the EU-Japan networking session that takes place on 27 September 2012. You will find the relevant additional information at:

http://ec.europa.eu/information_society/events/cf/ictpd12/item-display.cfm?id=8435

2. **ICT-2013.10.2 EU-Brazil Research and Development Cooperation**. The topics for consideration include:

a) Cloud computing for Science;

b) Sustainable technologies for a Smarter Society;

c) Smart Services and applications for a Smarter Society;

d) Hybrid broadcast-broadband TV applications and services;

The funding scheme for the coordinated call with EU - Brazil is Small or medium scale focused research projects (STREPs) with an indicative budget of EUR 5 million (a similar budget for the call is expected from the Brazilian Ministry of Science, Technology and Innovation (MCTI). The timing for the call is 10 Jul – 24 Oct 2012.

NOTE: The deadline for ICT-2013.10.2 EU-Brazil Research and Development Cooperation call has now been extended until 7th February 2013 and more information can be found at

https://ec.europa.eu/research/participants/portal/page/cooperation?callIdentifier=FP7-ICT-2013-EU-Brazil#wlp_call_FP7

The Horizontal International cooperation actions available in WP2013 include Objective ICT-2013.10.3 International Partnership Building and Support to Dialogues, where the goal is to support dialogues between the European Commission/the EU and strategic partner countries and regions, and to foster cooperation with strategic third country organisations in collaborative ICT RTD both within the EU's Framework Programmes (FP7, Horizon 2020) and under relevant third country programmes. The Targeted countries/regions include:

a) ACP countries (in particular Africa)

b) Asia (in particular China, India, South-East Asia)

c) Eastern Europe and Central Asia

d) High Income Countries: Subgroup 1: North America (Canada, USA)

e) High Income Countries: Subgroup 2: East Asia/Oceania (Australia, Japan, Korea, New Zealand, Singapore, Taiwan)

f) Latin America

g) Mediterranean Partner Countries

It is expected that each targeted area will be covered by at least one project, and that duplication of effort in an area is avoided. The Funding scheme/expected budget is Coordination and Support Action (CSA) (SA) with €8 million (maximum EU grant of EUR 800 K per proposal). The date of publication of Call 10 is 10/07/2012, call deadline: 15/01/2013.

References

[1] BIC Working Groups Workshop report http://www.bic-trust.eu/events/bic-workshop-on-the-cross-domain-coordination-of-international-cooperation-day-1-and-technical-themes-in-trustworthy-ict-and-inco-day-2/

The full presentation can be found at http://www.bic-trust.eu/files/2012/10/OLIVEIRA_BIC27Nov2012.pdf.

A2. Annex 2. Success metrics and impact (from June 2012 workshop)

At the June 2012 BIC workshop [4], there was an extensive session on the determination and identification of "success metrics" for international cooperation and collaboration and an agreed approach to come up with measures for success for this. This annex contains the results from this workshop.

Some noteworthy comments made during the presentations regarding success metrics were the following:

- It is difficult to predict the future; research on several topics is just a way to be prepared for the unknown future;
- 'Things happen' as a result of our activities but it isn't always clearly identified as a direct result;
- Measures for success should include rationale – motives and goals – for active engagement in international cooperation;
- Although difficult, as a working group already engaged in these activities, we could try to draw up some success criteria regard to results and monitoring;
- It would be useful for us as a community to agree on ways to carry out analysis and assessment of INCO impact.
- During the discussions, a number of points were discussed and agreed by the participants:
- Setting up multi-lateral international cooperation is not an easy endeavour as the countries all have different ways and mechanisms for carrying out Research and Technological Development (RTD) management, funding, plans and implementations, which are inherently difficult to set up (vision, interests, meetings, agendas). Furthermore, it takes a considerable amount of time, effort and patience to set up fruitful examples of INCO on a bi-lateral basis and even more complications on a multi-lateral basis. Therefore, the establishment of success metrics and measures will subsequently be as difficult with all of the factors involved. A clear example of this could be success could be garnered in one country but would then be classified as a failure if another country couldn't stand up to their side of the agreement due to some unforeseen reason.
- There were a number of ways to cooperate on an international basis. There could be a focus on Research / Dissemination & Exploitation activities (Academic interest/ industry). This is made complicated because some countries only focus on academic and research institutes whereas others have a stronger focus on industry funding; local/regional topics versus global cooperation topics in which there are calls open for specific topics, sometimes cooperation is needed for other topics not in open EU calls, which makes it very frustrating for the research communities. There is a need for more cooperation at the government and policy levels and not only at the research levels.
- How to measure the impact of INCO? The success metrics should be broken down at the various levels, e.g.
    - Market: business done, what has been exploited/how, number of companies created, new research plans, etc.;
    - Knowledge gained: specifications, new standards, new technologies;
    - Regulation, Policy: exp. new directives for Europe;

  - Others TBD.
- When thinking about metrics, would INCO for Security, Trust & Privacy RTD have special or different properties or considerations that make INCO
  - more important?
  - more difficult?
- We must think at a global level as there are key questions and there are notions related to security, trust and privacy have different meanings in the EU (South/North) as well as in third countries e.g. India/ Japan / China (with regard to cultural aspects). Scalability is also very important (e.g. China, India: >1 billion people for ID card) and cultural aspects e.g. the take up of biometrics where photography is involved.
- For topics like identity management, the research communities need to be talking at an international level: necessary to understand what identity means in Japan, China, India, etc… A similar argument has to be made for dealing with cyber attacks / hackers have different behaviours depending upon geography, legislation and culture. It must be taken account that some security topics cannot be shared easily e.g. geostrategic, exchange of data, and ways of incentivising this must be discussed.
- We need to determine how success can be measured in terms of contributions to multi-disciplinary research and technological development. What are the specific S&T issues and RTD challenges that must be addressed in a global context. A measure of success depends on a number of influential factors, including where the starting point is (whether a new collaboration or a more mature collaboration of long standing and the audience, whether they be the European Commission, the research communities, industry members, or other parties willing to engage in international cooperation.
- There is a tendency for people to only pay attention to the entities e.g. projects, initiatives, platforms, … that bring in the 'big bucks'. However, there could be some unsung heroes involved in these awards who don't get the recognition. Therefore, there is a need to have qualitative as well as quantitative evidence included in our measures of success.
- What should projects like ours measure? If you want to measure your results, outputs, deliverables, contacts made, … on a range from 1 to 10 grid, then you want to know about each of these items for the kinds of collaborations and influencing factors as mentioned above (maturity level and audience). How to characterise the things to measure is not altogether clear. It was suggested that a questionnaire could be sent to all the projects to try to identify the measurement items with weighting for each. It is difficult to measure the kinds of things being asked for as it is difficult to predict the future and 'things happen' as a result of our activities but it isn't always clearly identified as a direct result. A number of cases were discussed during the workshop where project participants learned of new projects spawned as a result of their projects many years afterwards.
- How do we measure non-scientific aspects (the ability to effectively network and eventually collaborate) along with more scientific aspects e.g. forming successful research proposals that pass the ever lowering barrier of success rates.
- How / when do you find the actual number of proposals / projects that were put together based on your earlier work. It is quite difficult to get all of the information on submitted proposals and even if you get these, how do you know they originated from your earlier work?

- We should clarify the purpose of these measurements, whether it be to develop the strategy for increased international cooperation or to justify the need for international cooperation projects (we believe it is the former mainly and that should be our focus).
- Is there a way to measure the change in number of non EU partners over time (numerator)?
- Measures of success should incorporate the rationale – motives and goals – for engagement in international cooperation, success criteria with regard to results and monitoring; and, finally, analysis and assessment of INCO impact.
- Would there be a way to calculate the amount of money that could be saved by engaging in international cooperation. For each topic area, are there any measures that could be realised e.g. it was suggested a good example could be international cyber security research, which could save the countries xyz euros if done together? Is it possible to put a number on how much is saved by involvement of international partners?
- Is there a way of distinguishing what makes sense of doing it alone in the EU and what makes sense carrying out on an international scale? Can we find out definitively which makes more sense? It depends on the research topic is and what resources are required for the research. Although we all believe it is important, due to many of the points raised above, it is difficult to quantify the benefit of international cooperation. We should work on this together to at least try and find this out in the future.
- Do we start by measuring the past? Or just start in the future? Do we start measuring new international cooperation beneficiaries. Also, should we measure the number of beneficiaries with whom you consult but then don't achieve success due to other factors outside your control? E.g. no interest in collaboration or funding isn't an issue in their own countries.
- Is it possible for us to measure Return on Investment (ROI)? In order to do this, we would need to measure utilization with some degree of precision. Although it is important to monitor where the money is being spent, you really want to measure increased productivity and effectiveness, but let's set that as an aspirational goal. During the workshop, we tried to capture a number of stories anecdotally about how consortia where formed (examples in EU-Africa, EU-India, EU-Australia, EU-United States).
- How would we go about calculating ROI from international community involvement (e.g., in FP7 and H2020)? Can we each contribute to how we could agree to quantify the benefit of international community involvement. A suggestion was made to create a success metrics survey to ask some of these questions.
- Perhaps measure the amount of collaboration with academic and industry in a region and try to quantify the role this has in sparking innovation and as serving as a catalyst within private industry, including the potential for a number of start-ups.
- We spoke about extended working groups and outreach to other interested parties. Is there a way to measure the success of these undertakings (no. of meetings held, topics/themes generated, visitations made, awareness, training and teaching courses held, consortia being formed, …?). However, we should not be placed in a position to measure items that will deliberately make our cooperation(s) look bad. In other words, it's a useful measure if you're trying to improve the community building mechanisms and not to destroy them.
- Is there a way to measure retention rate–how many of the community remain over a particular period as opposed to transient members who get involved once or twice.

However, we must be careful that we don't categorise transient participants who use the resources for a short time in a way to count them as failures. There could be mitigating circumstances where their research was carried out successfully and there was no further need to collaborate. This should, therefore, be classed as a success.

- Is there a way to measure excellence in an impartial way? In other words, how can actions that are supposed to be impartial separate excellence from mediocrity if encountered in the process?
- A participant (from India) suggested a tool could be customised for indicating metrics for success of international cooperation. This would be taken up following the workshop as the first step would be to get the participants to highlight the measures for success and give them appropriate weights. The tool could then be designed according to these.
- We should examine why some countries seem to have more of a success rate e.g. Australia and New Zealand. Could it be true that it was because they did/didn't need the resources.
- Reference to the on-going tools, based on technology platforms should be included, as they are mechanisms to foster the networking and cooperation between high level researchers and international partners are invited to join. The success case of the technology platforms as built for some Latin American countries represent a valid reference for other actions with other regions.