D4.2 BIC Annual Forum and IAG meeting

Grant Agreement number:	**258655**
Project acronym:	**BIC**
Project title:	**Building International Cooperation for Trustworthy ICT: Security, Privacy and Trust in Global Networks & Services**
Funding Scheme:	**ICT Call 5 FP7**
Project co-ordinator:	**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**
Revision:	**Final**

Project co-funded by the European Commission within the Sixth Framework Programme (2002-2006)		
Dissemination Level		
PU	**Public up to and including Annex III**	
RE	**Annex IV (IAG meeting minutes)**	

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

1st Annual Forum
29th November 2011
Brussels, Belgium

BIC Partners

BIC is a Coordination Action Project within the European Commission, DG INFSO Unit F5, Trust and Security
Jan. 2011—Dec. 2013

http://www.bic-trust.eu

Table of Contents

EXECUTIVE SUMMARY

The EU FP7 BIC project[1] held its first Annual Forum on 29th November 2011 in Brussels. The main goal of the BIC Co-ordination Action project is to engender co-operation of EU researchers and program managers with their peers in emerging countries, namely Brazil, India and South Africa**.** The project is facilitating a technical and programme level catalyst for engagement, collaboration and networking activities internationally. In addition, the BIC project will provide continuity and bring together a truly global collaboration with the participation of the already established countries from the INCO-TRUST project, including the United States, Canada, Japan, Korea and Australia. One of the means in accomplishing this ambitious goal is the holding of a BIC Annual Forum on Trustworthy ICT.

The **mission** of the BIC annual forum is discussion and agreement on technological challenges/gaps of common interest amongst the countries, agree on what can and needs to be done internationally (who can contribute to what), and then work at an international level towards delivering on cooperation towards solving these joint technological challenges. The forum will enable the working towards the definition of tangible international activities, including success metrics and setting up global projects.

The **objectives** of the BIC Annual forum are:

- Identification of the technological challenges that really need and could be tackled in common between the countries so they can be elaborated clearly with the policy makers in the respective countries as a way forward;
- Highlighting the current bi-lateral (and potentially overlapping) country to country cooperation(s) into a more comprehensive unified global cooperation;
- From the insights of the researchers and programme managers, to explore how best to organise future International cooperation (INCO) research activities and its supporting programmes, together with the key challenges, issues and priorities.

Significant **momentum** amongst the participants to build an international research community focussing on mutually beneficial research topics in trust, security and privacy was noted throughout the forum. There was a strong message from the participants to forge ahead with the necessary cooperation towards building the communities around the identified thematic areas of priority from their countries. Hence, an important outcome of the Annual Forum was the establishment of three working groups (WGs), two technical and one logistical, that would be facilitated by BIC. It would be the intention of the BIC project to additionally form longer term action groups based on the successful outcomes of these WGs to ensure implementation and take-up. The established WGs are entitled: WG1. Human oriented/citizen security; WG2. Network Information security / Cybersecurity; and WG3. Programme/funding focus/ identify community.

The full report of the BIC Annual forum contains a high level summary of all of the results from the sessions; detailed summaries of the presentations can be found in the Annex II of the report. The full report of the BIC Annual forum planning session held in July 2011 during the SysSec workshop can be found in Annex III. In addition, Annex IV contains the minutes of the IAG inaugural meeting that was held immediately after the BIC Annual forum on 29th November 2011.

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

INTRODUCTION

The EU FP7 BIC project[2] held its first Annual Forum on 29th November 2011 in Brussels. The main goal of the BIC Co-ordination Action project is to engender co-operation of EU researchers and program managers with their peers in emerging countries, namely Brazil, India and South Africa**.** The project is providing a technical and programme level catalyst for engagement, collaboration and networking activities internationally. In addition, the BIC project will provide continuity and bring together a truly global collaboration with the participation of the already established countries from the earlier INCO-TRUST project that included the United States, Canada, Japan, Korea and Australia. One of the means in accomplishing this ambitious goal is the holding of a BIC Annual Forum on Trustworthy ICT.

To prepare for the Annual forum, a BIC session[3] dedicated to the planning of the forum was held in Amsterdam on 6th July 2011 during the SysSec workshop[4] in which a number of topics were already identified for inclusion that were carried forward to the agenda. The full report of the planning session can be found in Annex III. In addition, Annex IV contains the minutes of the IAG inaugural meeting that was held immediately after the BIC Annual forum.

MISSION AND OBJECTIVES OF THE ANNUAL FORUM

The overall mission and objectives of the BIC annual forum are to bring together the wider and global trust and security communities to explore how best to organise future International Cooperation (INCO) research activities and its supporting programmes, together with the identification of the key challenges, issues and priorities to tackle together. The agenda was formed to cover the core objectives of the Annual Forum.

Objective 1. *Identification of the technological challenges that really need and could be tackled in common between the countries so they can be elaborated clearly with the policy makers in the respective countries as a way forward;* This objective was being covered by a presentation on identification of advantages for INCO and the trust and security technological challenges – BIC review of research topics already identified; and panel session 2: Human oriented approaches to security, privacy and trust and how international cooperation can benefit; and panel session 3. Digital ecosystems network and information security and how international cooperation can provide mutual benefits.

Objective 2. *Highlighting the current bi-lateral (and potentially overlapping) country to country cooperation(s) into a more comprehensive unified global cooperation;* This objective was being covered by the opening session on Setting the scene with DG INFSO views onINCO and Panel session 1: Other INCO-related projects with direct or indirect linkages to ICT trust and security aspects.

Objective 3. *From the insights of the researchers and programme managers, to explore how best to organise future International Cooperation (INCO) research activities and its supporting programmes, together with the key challenges, issues and priorities.* This objective was being covered by Panel session 1. Other INCO-related projects with direct or indirect linkages to ICT trust and security aspects; and panel session 2. Human oriented approaches to security, privacy and trust and how INCO can benefit; and panel session and 3. Digital ecosystems network and information security and how INCO can provide mutual benefits; and the closing session on planning and operations.

[2] http://www.bic-trust.eu/
[3] http://www.bic-trust.eu/events/event/bic-session-syssec-workshop/
[4] http://www.syssec-project.eu/events/1st-syssec-workshop-program/

AGENDA

9:00 **Welcome and Introduction**
Jim Clarke, Waterford Institute of Technology, BIC Coordinator

9:10 **Setting the scene with DG INFSO views on International Cooperation.**
Alvis Ancans, European Commission, DG INFSO, International Relations Unit
Gustav Kalbe, European Commission, DG INFSO, Deputy Head of Unit F5, Trust and Security

10:00 **Panel session 1. Other INCO-related projects with direct or indirect linkages to ICT trust and security aspects.**
Projects (Panelists): EU – India Spirit (Tom Williamson), Synchroniser (Katja Legiša), EURASIAPAC (Fernando Kraus Sanchez), SECFUNET (Marcelo Pasin), BILAT/ACCESS4EU/SECAS (Rado Faletic).

10:30 **Identification of advantages for international cooperation and the trust and security technological challenges – BIC review of research topics already identified.**
Michel Riguidel, Telecom Paris-Tech, ENST, France

11:00 **Coffee and networking break**

11:30 **Panel Session 2. Human oriented approaches to security, privacy and trust and how international cooperation can provide mutual benefits.**
Chair: Priscila Solis Barreto, University of Brasilia, Brazil
Panellists: Karima Boudaoud, France; Ioannis Krontiris, Germany; John Zic, Australia;
Jan Eloff, South Africa; Fabio Martinelli, Italy.

13:00 **Lunch break**

14:00 **Panel Session 3. Digital ecosystems network and information security and how international cooperation can provide mutual benefits.**
Chair: John C. Mallery, MIT, USA (for Karl Levitt, University of California, Davis, USA)
Panellists: John C. Mallery, USA; Bart Preneel, Belgium; Abhishek Sharma, India; Hiroyuki Hishinuma, Japan; Razvan Gavrila, Greece.

16:00 **Coffee and networking break**

16:30 **Planning and operations session**
Moderated by BIC partners

17:30 **BIC Annual Forum closing**

RESULTS OF THE ANNUAL FORUM

This section will summarise the results of each of the individual sessions. Please note that an extended outline of the individual talks can be found in Annex I. The presentations themselves can be found at http://www.bic-trust.eu/events/event/upcoming-event-bic-annual-forum/.

Taking into consideration the mission, objectives and inputs received for the annual forum, the programme was designed in a way to include a good mix of presentations, panel sessions and discussions. In summary, the programme outcomes consisted of the following elements.

The opening session of the Forum was an opportunity for the European Commission, in particular, **Alvis Ancans,** DG INFSO, International Relations Unit and **Gustav Kalbe,** DG INFSO, Deputy Head of Unit F5, Trust and Security, to set the scene for the BIC annual forum and present perspectives on INCO between the EU and other countries in the context of the ICT theme of EU's 7th Framework and the importance of INCO within ICT Trust and Security research. As part of this session, there were details presented on past, current and future activities in the pipeline already identified that are directly or even indirectly related to trust and security. During these two talks, the following points were highlighted:

- The Commission recognises the strong need to cooperate internationally, with the following objectives:
  - To jointly develop ICT solutions to major global societal challenges;
  - To jointly respond to major global technological challenges by developing interoperable solutions and standards;
  - To improve scientific and technological cooperation for mutual benefit.
- There are a number of targeted EU – Japan calls open presently in calls 8 and 9
  - Objective ICT-2011.1.1 Future Networks (Call 8);
  - Objective ICT-2011.1.2 Cloud Computing, Internet of Services and Advanced Software Engineering (Call 8);
  - Objective ICT-2011.3.1 Very Advanced Nanoelectronic Components (Call 8);
  - Objective ICT-2011 9.6 FET Proactive: Unconventional Computation (UCOMP) (Call 8);
  - Objective ICT-2011.5.2 Virtual Physiological Human (Call 9).

It is expected that there will be further joint calls in Work Programme 2013 that is under construction, including Brazil, Russia (currently under discussion; topics: high-performance computing and semantic web) and the possibility of coordinated Calls with Australia, South Africa, Mexico and Japan are in the pipeline – more likely in 2013.

Panel session 1. Other INCO-related projects with direct or indirect linkages to ICT trust and security aspects.

A panel session was comprised of a number of INCO-related projects with direct or indirect linkages to ICT trust and security aspects. The session was supported by the following projects - panellists:

Euro-India SPIRIT[5] project - Tom Williamson, European Research Consortium for Informatics and Mathematics, European Economic Interest Grouping) ERCIM EEIG. He is the project co-Ordinator of Euro-India SPIRIT project.

SYNCRONISER[6] project - Katja Legiša, an Italian consultant with seven years of experience in international and EU project management, promotion and support of research and development activities. Her professional and educational background is in Project Management, Public Relations and Communication. Since 2006, she is coordinating EU-India projects. She is now the Project Coordinator of the SYNCRONISER project.

EURASIAPAC[7] project - Fernando Kraus Sanchez, Director of the Foreign Affairs Sector within the Research and Innovation division of AToS in Spain. Fernando has over fifteen years of experience in participating in the implementation of ICT projects including the EURASIAPAC project. He has wide experience in the field of exploitation and marketing activities as a senior consultant both in the private and public sectors of different countries (Argentina, Azerbaijan, Brazil, Cameroun, Dominican Republic, Egypt, ..).

SECFUNET Project - Marcelo Pasin, Assistant professor at the University of Lisbon. Previously, he was a researcher at INRIA (France, 2007-2008) and tenured associate professor at the Federal University of Santa Maria (Brazil, 1991-2007). He has worked for CoreGRID, EGEE and EC-GIN in FP6, and is now working for TClouds and SECFUNET in FP7. SECFUNET is a project from within the recent EU-Brazil joint call held during Call 7 of FP7.

FEED/AUS-ACCESS4EU/SECAS - Rado Faletic's involvement with the Forum for European-Australian Science and Technology cooperation (FEAST) stems from his interest in promoting, encouraging and highlighting science and new ideas, along with the personal satisfaction he receives from facilitating individual collaborations.

The purpose of this session was to broaden the perspectives and to gain insights from other projects related to both INCO and trust and security. The format of session was the panellists were asked interactively to address key questions by the moderator and any other questions from the audience.

The following tables contain a condensed summary of the responses to the questions raised to the panellists (full responses are detailed in Annex II):

[5] http://www.euroindia-ict.org/
[6] http://euroindiaresearch.org/synchroniser/
[7] http://eurasiapac-fp7.eu/

Question 1	**How does your project contribute to International cooperation <u>and</u> trust and security?**
EU-India Spirit	• EU – India collaboration with working groups in ICT Addressing Societal Challenges; AudioVisual Media & Internet; and Emerging Technologies & eInfrastructures. • Trust and security: strong topic in all three working groups and hence, one of the umbrella themes.
SYNCRONISER	• Boosts impact of the policy dialogue by identifying EU-India research priority areas and recommendations on how to improve the cooperation. • one of identified research priority areas is *Security, Privacy & Monitoring* (data management system, secure storage system, person identification and tracking systems; for healthcare, governance and education).
EURASIAPAC	• Eurasiapac focuses on ICT research cooperation between the EC and the Asia-Pacific region, mainly Korea, Japan, Australia and New Zealand. • Trust and Security has been identified as one of the priorities among the topic of interest in ICT research in the countries participating in the project.
SECFUNET	• SECFUNET is a STREP in FP7, with EU and Brazilian partners. • It proposes to create a new generation in the Internet security that is very simple to use.
FEED/ AUS-ACCESS4EU/ SECAS	• *SECAS: Strategies for European ICT RTD Collaboration for Australia and Singapore* identified ICT thematic capabilities and areas of potential synergy, performed policy analysis and has made strategic recommendations for improved cooperation policies. • Trust and security topics are clearly identified in the final report, which is now available online.

Question 2	**What are the benefits and expected impact to your project brought on by international cooperation?**
EU-India Spirit	• The Indian partners have increased visibility and familiarity with Commission-funded projects, in particular, and EC processes in general as well as strong relationships with consortium members and related entities.
SYNCRONISER	• The project has provided a more practical, consultation approach to boost the impact of policy dialogues on Joint research priority areas. This will feed into the upcoming High level working group meeting in 2012. • Synchroniser uses a bottom up approach in which the project provides the EC with the evidence from the experts, on which they can make policy decisions.
EURASIAPAC	• The contacts and the fact that some main stakeholders in ICT research have been directly involved in the project has raised interest in launching joint calls with some of the countries. • Joint calls with Japan and Australia are under preparation and are being considered for the future.
SECFUNET	• SECFUNET's partners are very heterogeneous providing different yet complementary skills. Specifically from Brazil we get different perspectives, very different regulation frameworks and very different concerns and Brazilians also include a pioneer researcher in intrusion-tolerance and a national networking research laboratory. • SECFUNET also allows for leveraging previous cooperation, that would otherwise be impossible.
FEED/ AUS-ACCESS4EU/ SECAS	• Both FEED and AUS-ACCESS4EU have greatly contributed to the flow of information between Europe and Australia regarding overall funding modalities available for international collaboration, but more importantly have identified and developed strategies on how to most successfully use these mechanisms (including FP7, COST[8], ARC[9] and NHMRC[10]). SECAS has produced a concrete set of strategic recommendations, which are available in the final public report online.

[8] http://www.cost.eu/
[9] http://www.arc.gov.au/
[10] http://www.nhmrc.gov.au/

Question 3	**International cooperation is not an easy task and requires a lot of patience and time. What are the issues encountered and how did you address them?**
EU-India Spirit	• Difficulties in scheduling and organising face-to-face meetings are obviously magnified in international cooperation projects with such significant scale; • When involving external experts, need significant advance notice time for stakeholders.
SYNCRONISER	• The difference of viewing time and deadlines is different between the two countries, which brings to difficulties in carrying out joint activities. • The difference between Formal and Informal communications plays an important role in getting things done and especially when passing a message across.
EURASIAPAC	• Although the Eurasiapac project focuses on ICT cooperation between EC and the Asia-Pacific region, it's difficult to deal it as a homogeneous region because each participating AP country (Japan, Korea, Australia, New Zealand) has different characteristics, institutions and approach to ICT research. • In Europe, the EC FP7 creates a common approach to research, but it doesn't exist a similar common institutions in the Eurasiapac targeted countries. Each country needs to be dealt in a different way. • difficult working cooperation process due to time zone differences. • IPR is always an issue in international ICT research cooperation and needs to be dealt at a very early stage of the research process.
SECFUNET	• In time scales, although evaluated at the same time, the start times of projects were very different (by 6 months) and this caused significant start-up problems between the countries. • Cooperation projects in Brazil are not structurally the same as in EU. Brazilians operate in a more independent fashion and don't over-rely on meetings as we do in the EU. • The evaluation process is also very different between EU and Brazil. In Brazil, reporting is carried out mainly in the very end of the project, therefore, making it difficult to get things going in terms of a common progress reporting mechanism between the countries. Another example is Brazilians are not responsible for delivering to the EC. • These efforts need to be harmonised between the participants in the different countries.
FEED / AUS-ACCESS4EU/ SECAS	• One of the issues of most importance has been the persistent lack of understanding, particularly in Europe, regarding how to include third country partners on FP7 proposals. • FEED and AUS-ACCESS4EU have been working actively (through email alerts, but more affectively through targeted seminars and direct communication) to education both Australian and European researchers on *the facts* as well as *the realities* of including Australian partners on FP7 projects. This includes issues of funding support. • SECAS has identified issues ranging from abstract political ones (e.g. that policies need to be concrete, should also include technical content, and need follow-up actions) to practical ones at the researcher level (e.g. how to best work over long distances, the benefits of setting up joint labs, the challenges of researcher exchange, etc.).

Question 4	**In the opening session, it was mentioned by the Commission that INCO projects should go further than just identifying stakeholders and who the counterparts are in the countries and topics of cooperation. What are your projects plans to take this approach for a longer term strategy and is there anything that BIC can do to help you with this strategy?**
EU-India Spirit	• The EU – India Spirit project is finishing at the end of December 2012 so it is difficult to plan a longer term strategy beyond this and it hasn't been built into the legacy planning. • In terms of BIC, it is highly recommended to continue the collaboration in the countries and it has been a highly mutual benefit to have a number of the BIC members involved in the working groups of EU – India Spirit from the very start.
SYNCRONISER	• Both the EU – India Spirit and Synchroniser projects have had long term planning problems due to the periodic postponements over the last 2 years of the main DIT/EU meeting. However, this same situation resulted in this very topic of long term planning to be included as a key recommendation being made by the project. • For liaising with other projects like BIC, this is also included in a recommendation that the follow up work can be directly or indirectly supported by other projects and/or other initiatives or channels. • Recommendations on improving the longer term cooperation between the countries via other means apart from the projects as projects have limited duration. Some examples in discussions include: Executive bodies, collaboration with EU based eTPs, forming India based eTPs, which would be discussed in more detail later. This approach came up as the project recognises that research priorities have a strong tendency to change from year to year and we need something more everlasting. This is what is missing now and needs to be addressed as a matter of urgency.
EURASIAPAC	• This is an issue that was highlighted and attempted by EURASIAPAC also but it was found to be incredibly difficult as even though the project's overall goal was to consider the cooperation between the EU and the entire ASIAPAC region as a whole, in actual fact, there are considerable differences between the countries involved and these always need to be factored into the discussions and cooperation models. • Therefore, a bi-lateral approach is absolutely necessary even if there are some common cooperation issues across the regions.
SECFUNET	• As a perspective for longer term exploitation, as it is a STREP project carrying out RTD that will have eventual exploitation value, SECFUNET have several industrial partners. We feel it is the combination of the companies that are going to do their development of their products within the projects in order for the project to have a longer term impact for both the partners and the project in general. • Examples: Twinteq wants to develop its products in near-field communication, EtherTrust and Implementa work with secure elements like SIM cards, and Infineon wants to boost its trusted components for the future networks. More generally, SECFUNET wants to establish a sound security infrastructure that could be used by anyone.
FEED / AUS-ACCESS4EU/ SECAS	• The issue of sustainability has been a very important one especially within the FEED/BILAT projects where they have started working already with what we call 'multipliers' to impart our knowledge and key ideas around Australia. For other projects, it is an issue. What can projects do during their lifetime so the work can continue? BIC can talk to the SECAS project to see if there is anything BIC can do to help create this value. • BILAT project, one of which just finished are putting together significant workshops on specific topics. BIC can help develop the content and identify the individuals who can contribute to this workshop. This can lead to more lasting co-operations.

Question 5 What are your recommendations for improving effectiveness?

EU-India Spirit	• Greater emphasis should be placed on widening the net of participating international partners, so as to ensure that consortia are to the greatest extent possible comprised of partners with the most appropriate competencies and not the limited pool of potential partners who are already familiar with the FP7 structure and have previously participated in projects. • In this regard, projects promoting international cooperation such as BIC, India-Gate and its equivalents for the other BRIC countries are crucially important.
SYNCRONISER	• Recommendations include setting up collaboration with ETPs and xETP Initiatives in order to launch the Indian Technology Platform Channel. • Recommendation to involve Indian experts in the ISTAG related activities: Search on the mechanism which would allow Indian experts to get involved in the relevant bodies shaping priorities and strategic directions of the FP7/Horizon 2020. • Another recommendation is to establish a JWG Action Group for executing JWG outcome: Proposal to establish a JWG Action Group that could execute the JWG outcome. The form could be flexible (nomination of officers by EU and India, Support Project, Tenders, ...). The Action Group would be a sort of executive office to undertake the decisions adopted by the JWG. • Another recommendation is a proposition of a Co-funding Model for DIT: *Analyse Energy and Biotechnology co-funding programmes (between EC & DST).*
EURASIAPAC	• Recommendation to create more agile processes to define, launch and approve ICT cooperation initiatives. Many of the Asia-Pacific institutions involved in the projects, mentioned that the period of time to create, prepare and launch a cooperation initiative should be shorter as the view is that EC processes take too long. • Understanding legal and administrative EC funding processes are not always easy for non EC institutions; simplified methods may enhance international participation.
SECFUNET	• As recommendations for improving effectiveness, better agreements with non-European authorities, with, for instance, better definitions in the commitments, and better synchronisation. It could include previous negotiation for project management standards, as, for example, how to deal with deliverables, project review and evaluation. • The European Commission should help the targeted applicants to have knowledge of its rules and evaluation standards, using, for example, concertation meetings in the targeted countries.
FEED / AUS-ACCESS4EU/ SECAS	• Recommendation for better coordination and information-sharing between the variety of INCO activities across FP7. Consideration should be given to this issue in future INCO calls. • Recommendation that activities be developed to facilitate the integration of activities amongst all INCO projects, particularly so that findings can be directly implemented into ongoing projects (rather than waiting for final reports, which in any case are rarely read by other INCO actors).

Keynote Presentation: Identification of advantages for international cooperation – BIC review of research topics already identified.

In this keynote presentation, Professor Michel Riguidel presented the key technological challenges and themes already identified from within BIC thus far and previously within the INCO-Trust project[11]. These findings would be used as a benchmark later on during the discussions. During the presentation, a number of points were highlighted including:

- The need for the international ICT trust and security community to collaborate on identifying both strategic and tactical recommendations and priorities[12];
- Four main themes have been highlighted for INCO in trust and security:

Theme 1: Digital ecosystem security (Network & Information security) oriented to the System. This theme involves protection and trustworthiness with the strengthening of infrastructure resilience and control crisis management, crisis management (CIP), Security and cyber-defence (incl. against the asymmetric challenge). It also includes securing the current and Future Internet, network/system security, securing cloud computing for enterprises, Mobile security, security for mobile connectivity. In addition, it deals with policy properties such as variety, scalability, reciprocity, diversity, complexity and interoperability.

Theme 2: Trust & Privacy (including personal data protection) oriented to the Humans, Users. It incorporates topics related to responsibility (Identity versus Anonymity), designing identity and accountability management frameworks, international Privacy friendly authentication and reputation assurance. It includes measurement and negotiation, repositioning trust infrastructure at the same level as security infrastructure and trust management. Other areas under this theme include secrecy, dignity, sovereignty designing digital sovereignty and dignity, and new privacy infrastructures, reconsidering privacy spaces, storage function areas; and, last but not least, usability creating a Human oriented and usable security for citizens.

Theme 3: Global Framework & International alignment oriented to principles & governance. This includes properties such as interoperability, openness, transparency and secrecy; the preparation of policy frameworks to enable global collaboration and interoperability; Knowledge and International Data exchange architectures for cybersecurity; and socio-economic aspects including data policy, governance and secure, trustworthy and viable ecosystems.

Theme 4: Methodology, tools and technical challenges oriented to the tools. Under this theme is expertise sharing in science, technology & engineering; methods to support metrics and standardization issues; software security to enable the engineering of secure and trustworthy software and systems; protection of data and information with cryptology (digital signature, etc.) and other upstream topics including the initiation of green security.

In conclusion, Professor Riguidel presented a table showing a summary of all of the countries interactions to date, showing the programme/funding agency contacts, research level contacts and a sampling of the priority research themes for + INCO in trust and security. The full table can be found on the next page.

[11] http://www.inco-trust.eu/
[12] http://www.inco-trust.eu/media/D3_1_report.pdf

Summary of interactions between INCO countries to date, showing the programme/funding agency contacts, research level contacts and priority research themes.

Country	Program Level	Research level	Priority research themes for INCO
USA	National Science Foundation Department of Homeland Security	Massachusetts Institute of Technology, Rutgers University, University of California, San Diego, University of California, Davis, University of Illinois , Others	CyberSecurity/Privacy: Technology and Usage Issues Trustworthy International information exchange including data transfer and sharing, Security models for the Future Internet.
Canada	National Science & Eng. Res. Council	Univ. of New Brunswick, Ecole Polytechnique Montreal	Industry driven projects on trust, security and privacy.
Korea	Ministry of Knowledge Economy, KEIT	SoonChunHyang University, Seoul National Univ. Others	Internationalisation of data (identity management, privacy, end to end trust metrics, ...); Countermeasures against Massive DDoS; Security of Cloud computing e.g. Security of Smart Grid; Security compliance management and information security assurance; Security for VoIP and Mobile communications; Future Internet.
Japan	Japan Science and Technology Agency, CREST programme, MIC	NICT, University of Tokyo, Tokyo Inst. of Tech, JAIST, Others	Dependability, Security, Privacy and Trust of embedded systems
Australia	Australian Research Council (ARC)	CSIRO, NICTA, Macquarie University, Univ. of Sydney, IIS Partners, many others	Communications Security, Trust and Privacy in the Future Internet; Formal approaches for trust and security.; Sensor networks.
Brazil	CNPq (National Research council), FUNTEL, State Research foundations ITI (Instituto Nacional de Tecnologia da Informação)	Universidad de Brasilia, Univ. of Sao Paulo, CPqD Serasa Experian, Others TBD	Future Internet, Wireless Technologies: Security, Privacy, Trust over ad-hoc networks, Quantum crypto, ID management.
South Africa	SA Dept. of Science and Technology SA Technological Innovation Agency	Council for Scientific and Industrial Research (CSIR) – The Meraka Institute, SAP, University of Pretoria, University of Johannesburg, University of South Africa, others	Wireless Technologies: Security E-infrastructures security and trust
India	Dept. of Information Technology (DIT), ERNET, EuroSpirit India Support action (FP7)	India Institutes of Technology (IITs), India Institute of Science (IISc), Universities - Hyderabad, Pune, Anna amongst others).	Data Center Security, Data Privacy, ID card, ID management.

Panel Session 2. Human oriented approaches to security, privacy and trust and how international cooperation can benefit.

The panel session was supported by the following researchers/presentations engaged in the panel session topic areas.

- Karima Boudaoud, University of Nice, France: "Human oriented and usable security management"
- Ioannis Krontiris, Goethe University Frankfurt, Germany: "Privacy-respecting Authentication"
- John Zic, Commonwealth Scientific and Industrial Research Organisation (CSIRO) ICT Centre, Australia: "Human-oriented approaches to trust, security and privacy and the role of international cooperation"
- Jan Eloff, SAP Meraka UTD / SAP Research Pretoria, South Africa: "Collaboration with Africa / BRICS [13] for human oriented approaches to security, privacy and trust"
- Fabio Martinelli, Istituto di Informatica e Telematica - IIT; National Research Council - C.N.R., Italy: "Network of Excellence on Engineering Secure Future Internet Software Services and Systems"

Based on these presentations and discussions at the end of the session, a number of research items for Human oriented approaches to security and INCO were elaborated by the participants.

Multi-disciplinary International cooperation amongst all stakeholders

Security management should be more accessible to all kind of users and especially non-security experts evolving towards a more human oriented security management vision. To address today's security issues, we need to: 1) move from the traditional technology-only oriented design of security solutions towards user-centric security management and 2) bring together experts from psychology, social science, economics, legal, technologists and security experts to address security and privacy from a user point of view and put her/him at the heart of problem. From an international point of view, we need:

- Collaboration between security experts and experts from other disciplines (psychology, social science, etc.) and from different countries, in addition to collaboration with international government institutions.
- Organisation of **multidisciplinary** and **international workshops** targeting wide public.
- Set up of **multidisciplinary** and **international working groups** in targeted countries.
- Collaboration with international standardization organisations.

[13] BRICS group of countries: Brazil, Russia, India, China, and South Africa

Technological research can also greatly benefit from international cooperation when it comes to taking into consideration the human factors in designing technologies. The following questions should be examined:

- How people perceive technological solutions and how that affects the adoptability of the corresponding technologies?
- How to best explain to people the potentials and features of the existing solutions?
- How to best design user-interfaces to encourage usability and adoptability?

The answers to these questions will vary for different cultures and by opening up research beyond the European borders. It would give us a great insight in these aspects and eventually help us design better technology.

To address the above challenges, collaboration opportunities should allow EU-project consortia to open up and include various kinds of actors in the international setting: user communities, governmental organizations, regulatory authorities, and research institutes. A framework for enabling such collaboration should encourage joint working groups, organization of public events with experts from both sides and collaboration in standardization activities.

Privacy concerns in an international setting

Currently, European RTD projects engaged in privacy research e.g. ABC4Trust are building architectures based on privacy requirements collected within the European setting (e.g. Greece and Sweden). However, privacy concerns differ in the international setting. These differences can be attributed to differences in cultural values and perception of privacy, differences in the familiarity with Web privacy practices, or even differences in regulations. In that respect, international cooperation could greatly help exchanging views with other cultures, collect different application scenarios and requirements from other cultures and effectively broadening the perspective of privacy-ABC architecture.

Privacy and information utility are conflicting requirements. As the level of privacy increases, the level of information utility decreases. This is because as we hide more information to preserve privacy, the usefulness of the released information decreases. Local context and culture also influence what information should be regarded as private, and what information is considered as useful. It is, therefore, an open research question to be discussed how privacy relevant processing with and in countries like Brazil, India or South Africa can be handled within the European context.

- How are concepts like proportionality, unlinkability, minimal disclosure etc. being perceived in other countries?
- How other legal systems outside Europe can be affected by and have effects on Privacy-ABCs?
- How to ensure an optimum balance between privacy and utility, taking into account local contextual needs and preferences?

The establishment of "Path-finder" projects

Establishing international co-operation is important in two respects. First, it offers collaborating partners increased access to potential receptors for ideas and cross-fertilisation of markets. Second, by definition, it builds a larger research community, and this in turn can enable future, potentially larger/more complex collaborative projects in trust, security and privacy. However, alignment and commitment is required at multiple levels, from the individual researchers to their respective organisations and to the participating governments. This complexity should be in the first instance address in a methodical manner.

First, identifying partners who are like-minded and interested in addressing similar, relatively small scale but concrete problems with real needs (addressing the information management and process requirements of the bio-security communities in the EU and Australia was used as an example). These can be regarded as "Path-finder projects", which stand a good chance of being identified, proposed and finally supported by the broader community. Of course, any such project requires funding and commitment from each partner, and in the case of international co-operation, agreements need to be in place between the respective governments to allow the collaboration to proceed. This is particularly significant, as success requires the respective governments' policies and budgets to agree to participate in the international collaboration.

Actions that can be taken to build international co-operation include the development and building of local expertise and a community of users through such "Path-finder projects". The success of these is then used to promote further development of international collaborations to the broader community. Path-finder projects may also be used to build up international linkages on an incremental level, with the community of users developing internal and external trust in each other to be able to successfully work together. As part of the community building, the development and engagement of partners in formal forums (such as the Internet of Things Forum, for example) is very important, with regular face-to-face meetings (both formal and informal) occurring during these fora. Once again, as a part of the community building exercise, it is important that each potential partner is able to support the work through assuring some funding and resourcing is set aside specifically for this activity. Good will is necessary, but not sufficient, for ensuring a successful collaboration or community building exercise.

Secure software-services development

Security concerns must be addressed from the very beginning in system analysis and design, thus contributing to reduce the amount of system and service vulnerabilities and enabling the systematic treatment of security needs through the engineering process. In light of the unique security requirements the Future Internet will expose, new results will be achieved by means of an integrated research, as to improve the necessary assurance level and to address risk and cost during the software development cycle in order to prioritize and manage investments. To address this, the NESSoS project research covers

several main areas: A first set of activities represents the traditional early stages of (secure) software-services development: from secure requirements over architecture and design to the composition and/or programming of working solutions. These three activities interact to ensure the integration between the methods and techniques that are proposed and evaluated. In addition, NESSoS research programme adds two horizontal activities that span the service creation process: Both the security assurance programme and the programme on risk and cost aware SDLC will interact with each of the initial three activities, drive the requirements of these activities and leverage upon, even integrate their outcome; finally, notice that all 5 research activities mentioned above will be inspired and evaluated by their application in specific FI application scenarios.

NESSoS has set up a Networking and Liaison Board (NaLAB) for international cooperation mainly aimed at representatives of Technical WGs in the topics of the NoE. The creation of the NaLAB is in progress right now and it is explicitly meant to collect researchers from outside Europe. Several NESSoS components would benefit the international cooperation: the NESSoS Common Body of Knowledge; the engineering tool workbench; open competition, research activities. NESSoS plans to identify the main stakeholders in the NESSoS topics world-wide and create connections among researchers/WGs especially using the NESSoS internal mobility programme. Some possible cooperation topics include comparison of tools and techniques; usage control of disseminated data; and focus on SLA with protection of information, possibly in cooperation with other projects as ASSERT4SOA and ANIKETOS.

Research and technology outputs

International collaboration should be based on context awareness. Traditional user-centred approaches for technology development do not consider cultural and contextual needs. This results in deriving user requirements that do not give a correct view of the real needs, leading to technology shortcomings. Examples of contextual factors that should be considered include:

- Cultural norms and tradition
- Appropriate tactics for community entry and engagement
- Appropriate research techniques that involve the users and communities
- Appropriate needs assessment practices
- Infrastructure capacity of the targeted community
- Solution maintenance and life-cycle costs

The technology developed should be advantageous from the viewpoint of the local users. Therefore, technology development should be based on an understanding of the real requirements as well as an understanding how existing technology can be adapted to meet contextual requirements. Lastly, solutions developed should be relevant to local users, their needs and the available infrastructure.

Enhanced Collaboration methodology

European funding opportunities (e.g. Framework Programmes) should encourage collaboration with partners in Africa / BRICS. European Project consortia should be more open to accept African / BRICS partners, which should not just provide use cases, but should also develop and adapt technology for their local needs.

We also recommend the following three areas of research topics for international cooperation with regards to security, privacy and trust.

International approaches to usable security

In Africa / BRICS, mobile phones are the most common ICT device used. Typical users of such devices may not fully understand the security vulnerabilities the use of these devices pose. Security configuration of such devices for most users will therefore be a challenge. Therefore, the research challenge to address with regards to facilitating usable security is: How to quantitatively analyze and design appropriate user interfaces for mobile devices to enable a typical user to make informed decisions about different security settings?

International approaches to Trust

In African communities, trust is influenced by social network position. Social position governs activities within rural communities. For example, the chief of a village can influence business collaborations. Rural communities, therefore, require a different approach to business due to unique social structures, social norms, and traditions. Therefore, the research challenge to address with regards to trust is: How to ensure that trust management takes into account concepts relevant to the target context?

In conclusion, by facilitating international cooperation to provide human oriented approaches to security, privacy and trust, we believe that both European and African / BRICS partners will benefit. The great potential of the Africa / BRICS market can be exploited, while at the same time, these markets will be provided with solutions that are appropriate, affordable and contextually-relevant.

Panel Session 3. Digital ecosystems network and information security and how international cooperation can provide mutual benefits.

The panel session was supported by the following researchers/presentations engaged in the panel session topic areas.

- John C. Mallery, Massachusetts Institute of Technology, USA, "International Data Exchange and A Trustworthy Host: Focal Areas For International Collaboration In Research And Education"
- Bart Preneel, Katholieke Universiteit Leuven, Belgium. "International Cooperation in Cryptology"
- Abhishek Sharma, NetEdge Tele-Solutions (P) Ltd., India, "Trust and Security for Mobile Communications Services"
- Raznan Gavrila, European Network and Information Security Agency (ENISA), Greece, "EU-US joint CIIP Exercise, Cyber Atlantic 2011"

Based on these presentations and discussions at the end of the session, a number of research items for Digital ecosystems network and information security and international cooperation were elaborated by the participants.

International Data Exchange architecture for Cybersecurity needed

A key message is the acknowledgement that international cooperation in Cybersecurity is nascent and a more global approach is urgently needed because there is ultimately just one, single, global information environment, consisting of the interdependent networks of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. It is essential that we have the ability to conduct comprehensive intelligence collection and evaluation on any developing situation that threatens our cyberspace activity, followed by near-simultaneous processing, exploiting and disseminating of the information. This depends on collaboration, data exchange and sharing (and also knowledge sharing) between countries. We need comprehensive research towards international *intelligence*, *surveillance*, and *reconnaissance* (ISR) in the cyberspace domain.

The challenges can be characterized as follows:

- **Problem:** Attackers can replay attacks across different countries without rapid international learning to defend against attacker innovations
- **Benefits:** International collaboration and coordination can rapidly reduce defensive gaps across the OECD and build crisis-response capacities
- **Leverage:** Bias work factors in favour of defence and against cyber attack
- **Approach:** Exchange data related to cyber crime, attack patterns and best defence practices
- **Research:** Motivate technical research via needs of realistic data sharing scenarios

An architecture for international and cross-sector sharing of cyber threat and attack data will ensure a more effective collective cyber defense than countries, sectors or organizations might otherwise achieve individually. A strawman architecture for an international data exchange framework was presented that would enable the international cybersecurity community to securely carry out cyber data sharing and collaborative analysis as follows:

- Build shared awareness and understanding of cyber phenomena across countries
  - Employ shared data collection methodologies
  - Integrate measurements of phenomena across borders
  - Focus early on cyber crime and economic incentives
- Create comparable transnational data sets
  - Capture cyber breaches, attack patterns, best practices, defensive coordination
  - Include aggregate data on crime, black markets, economics, state-state interactions, long-term transformations
- Field a cyber data sharing framework that helps countries to:
  - Collect cyber data for compatible sharing
  - Fuse data to create common situational awareness
  - Manage national legal impediments to sharing via derived or aggregate data or by recommending harmonization steps
  - Exchange derived data in real time
  - Provide mechanisms for controlled drill down needed for law enforcement, advanced persistent threats (APT) or cyber emergencies
- Build shared collection, fusion, analysis, and response capabilities.

Open source trustworthy host platform for collaborative research and education

An open-source trustworthy host platform for collaborative research and education is required to address the following challenges:

- Problem: Attackers are subverting legacy architectures, which are inadequate for current threats
- Benefits: Development and evolution of a clean-slate trustworthy host will:
  - Create reference host architecture for computing, routers, cloud, embedded, wireless
  - Integrate best information assurance (IA) engineering from the open literature
  - Provide a reference paradigm for cumulative research and education
  - Drive higher assurance for open source and commercial software
- Leverage: Raise work factors required to compromise commodity hosts
  - Eliminate remote access penetration vectors
  - Prevent privilege escalation
  - Manage information leakage
  - Verify tool chain and resulting software

    - Rapidly detect and remediate flaws or breaches
- Approach: Pool research efforts across OECD countries to create and evolve a shared host platform reflecting best IA engineering practices
- Research: Motivate technical research via needs of an existing and readily-accessible free implementation.

International Cooperation in Cryptology

With respect to cryptology research on an international level, there is a need for integrated research and policy levels between the EU and counterparts around the world, and collaborative research is required across academia, industry and government agencies. To build an international strategy for INCO in cryptology, there is a need for collaboration on cryptographic algorithms with the establishment of open competitions with shared governance; effective standardization and continual updates of a key lengths and parameters document register (management of standards). Collaboration also should take place on cryptographic protocols motivated by distribution of trust and privacy (key component in privacy by design) and joint research also need to occur in these areas. We can be more effective by avoiding duplication and increasing impact on both the technology and policy levels. During the discussions, it was also pointed out that for the International open source trustworthy host platform presented, a common cryptographic software stack is a requirement agreed by everyone.

Mobile Security of Software Services

In future, significant confidential operations such as banking transactions and mail exchanging will take place largely from mobile devices. In these cases, it is vital to protect the customer data and applications from attack. Since the Smartphone/Mobile penetration is increasing globally, it makes a lot of sense that large regions, particularly regions like Europe and India/ Asia collaborate closely for the Research & Industrial Developments. Many companies are already putting effort in developing their goals and strategies for securing mobile data and applications.

Furthermore, it is critical to understand what there is to lose – the global vulnerability – before a major mobile security breach occurs. The ultimate goal is not about completely eliminating mobile security risks but rather having the proper systems in place to minimize the impact when breaches occur. Well thought out international controls involving the proper security technologies combined with the proper documentation and business processes are essential.

Mobile Security coverage of international technological research areas should include access, transmission, switching/ distribution, and storage. The international research communities should also focus on other related areas including policy, standards, tools, regulatory controls & test beds. There is already an Indo-Australia project covering international cooperation on mobile / wireless threats. It was suggested that this project should be examined and whether it could also include an EU element to it.

It was also suggested that the level of Industry participation may be increased from where it is and a higher mix of SMEs and large corporate with research bodies would be ideal. Towards this, BIC can be a key player in ensuring this critical coordination.

Joint exercises for Cybersecurity planning and improvement across borders

A presentation was made about the joint EU-US Joint CIIP exercise, called Cyber Atlantic 2011, co-organised by the European Union's cyber security agency, ENISA[14] and the Department of Homeland Security (DHS) in the USA. The first joint exercise was held on 3rd November 2011 and was set up as a centralised table-top exercise in which over 20 countries were involved (17 countries played).

Cyber Atlantic 2011 was an exploratory exercise with the following objectives:

- Explore and identify issues in order to improve the way in which EU Member States would engage with the US during cyber crisis management activities;
- Explore and identify issues in order to improve the way in which the US would engage with the EU Member States during their cyber crisis management activities, using the appropriate US procedures;
- Exchange good practices on the respective approaches to international cooperation in the event of cyber crises, as a first step towards effective collaboration.

There was a two part scenario used for the scenario:

1. Advanced Persistent Threat (APT) scenario with a hacker group, "Infamous", *exfiltrated* sensitive documents from EU and US – 'Euroleaks' web site and
2. Supervisory Control and Data Acquisition (SCADA) scenario highlighting vulnerabilities leading to backdoors (and failures) on Programmable Logic Controllers of power generation equipment.

The initial lessons learned (results ongoing) from Cyber Atlantic 2011 were:

- Mechanisms/structures for cross-border cooperation do exist; however, each country needs awareness of all communications options ;
- There is a further need to exchange Standard Operating Procedures (SOPs), training, exercises;
- Exercises need increased participation from all three areas: Technological, Law Enforcement, Policy/Political;
- Single Point of Contact in EU for US would help but is not compulsory;
- More exercises/workshops are needed!

[14] http://www.enisa.europa.eu/

CONCLUSIONS AND NEXT STEPS

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

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

Session 1: Opening session and panel of INCO projects.

James Clarke presented the recommendations from session 1:

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

Session 2: Human Oriented Approaches to Security.

Priscila Solis Barretto presented the recommendations from session 2:

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

- **Availability of Funding mechanisms:** good will is important but there must be a political work between agencies in the different countries to be successful.
- **Cooperation activities** to compare tools and techniques, avoid duplication, validation of case studies and shared testbeds **in different environments** and **cultures**.

Session 3: Digital ecosystem and network information security.

John C. Mallery presented the recommendations from session 3:

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

BIC Working / Action Groups

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

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

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

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

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

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

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

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

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

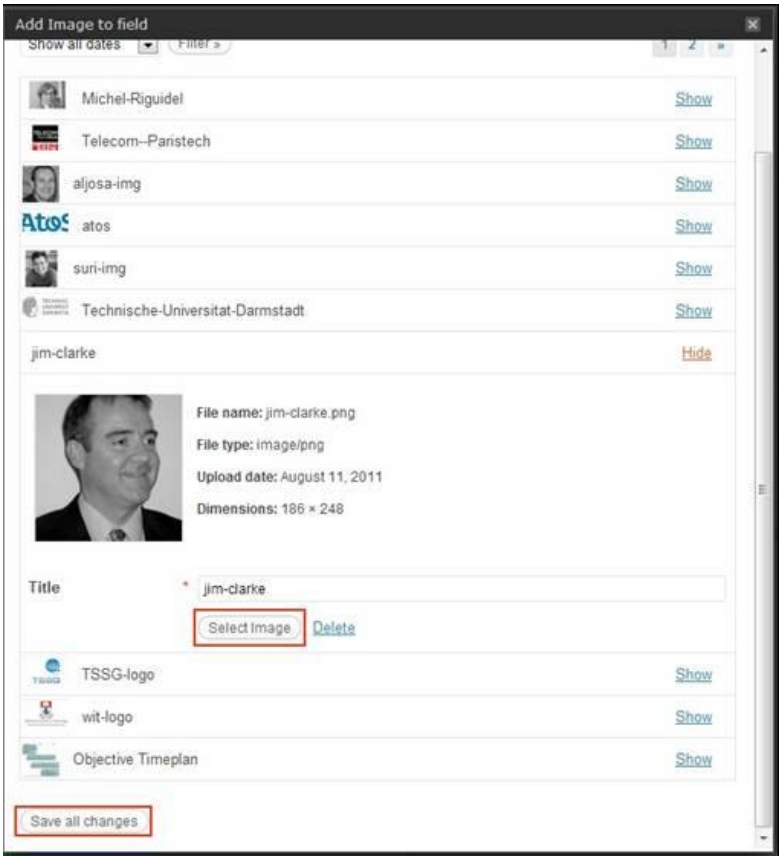

Figure 1. BIC Research network portal – data entry page

Acknowledgments

The BIC project is funded under Call 5 of FP7 ICT and began on 1st January 2011 with a duration of three years. The project is supported by the European Commission DG INFSO, Unit F5 ICT Trust and Security Research[15].

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

Annex I. List of registered attendees

		BIC Annual Forum Registrants as of 28th November 2011	
Last Name	**First Name**	**Organisation**	**Country**
Aguilar	Virginia	Nato	Belgium
Ancans	Alvis	European Commission	Belgium
Arsene	Vlad	Vector Business Consulting (RO)	Romania
Barreto	Priscila Solis	University of Brasilia	Brazil
Boudaoud	Karima	University of Nice	France
Bus	Jacques	DigiTrust.EU	Netherlands
Clarke	James	Waterford Institute of Technology	Ireland
Cleary	Frances	Waterford Institute of Technology	Ireland
D'Antonio	Salvatore	University of Naples Parthenope	Italy
Eloff	Jan	SAP Meraka UTD & University of Pretoria	South Africa
Faletic	Rado	Forum for European-Australian Science and Technology cooperation	Australia
Gavrila	Razvan	European Network and information Security Agency (ENISA)	Greece
Hishinuma	Hiroyuki	National Institute of Information and Communications Technology (NICT)	France
Hoepman	Jaap-Henk	TNO, Groningen & Radboud University Nijmegen	Netherlands
Howker	Keith	Waterford Institute of Technology	Ireland
Ishigami	Megumi	Fraunhofer IFF	Japan
Kalbe	Gustav	European Commission	Belgium
Kar	Ashok	Infra Technologies	France
Kechadi	Tahar	University College Dublin, Ireland	Ireland
Krontiris	Ioannis	Goethe University Frankfurt	Germany
Legiša	Katja	TESEO Sprl	Belgium
Levitt	Karl	University of California, Davis	United States
Mallery	John C.	Massachusetts Institute of Technology	United States
Malone	Paul	Waterford Institute of Technology	Ireland
Martinelli	Fabio	National Research Council - C.N.R.	Italy
Massonet	Philippe	CETIC	Belgium
McManus	Gary	Waterford Institute of Technology	Ireland
Menevidis	Aki Zaharya	Fraunhofer IPK	Japan
Morales	Stephanie	Sigma Orionis	France
Morgan	Gary	Commonwealth Scientific and Industrial Research Organisation (CSIRO)	Australia
NIVOLIANITOU	Zoe	NCSR 'DEMOKRITOS'	Greece
OLIMID	Cristian	European Commission	Belgium
Pasic	Aljosa	AToS	Spain
Pasin	Marcelo	University of Lisbon - FCUL	Portugal
Preneel	Bart	Katholieke Universiteit Leuven - COSIC	Belgium
Riguidel	Michel	Telecom-ParisTech, ENST	France
Sanchez	Fernando Kraus Sanchez	AToS	Spain
Sekiguchi	Satoshi	AIST	Japan
Sharma	Abhishek	NetEdge TeleSolutions Pvt. Ltd.	India
Skellern	David	Macquarie University	Australia
Sora	Adrian	Vector Business Consulting (RO)	Romania
Torrenti	Camille	Sigma Orionis	France
Tsagalidis	Ross W.	FMKE	Sweden
Williamson	Tom	ERCIM EEIG	France
Yuncken	Elizabeth	Commonwealth Scientific and Industrial Research Organisation (CSIRO)	Australia
Zic	John	Commonwealth Scientific and Industrial Research Organisation (CSIRO)	Australia

Annex II. Summary of presentations made at the Forum

The Annual Forum Welcome and Opening – James Clarke

Speaker: James Clarke, Waterford Institute of Technology, TSSG, Ireland

Since January 2011, James Clarke is Project Coordinator of a European Framework Programme 7 Co-ordination action entitled BIC, which stands for Building International Cooperation for Trustworthy ICT: Security, Privacy and Trust in Global Networks & Services. BIC will engage the European Union trust and programme management (funding organizations) and research communities with their peers in Brazil, India and South Africa and enable the collaboration with research communities in trust and security already established in the US, Australia, Japan, Korea and Canada established in the recently concluded INCO-Trust project that Mr. Clarke also coordinated from 2008 - 2010. In addition, Mr. Clarke is actively involved in the research community, having served in various international conference committees as organizing, technical and programme committee member.

Mr. Clarke opened the annual forum by describing the overall mission and objectives of the BIC annual forum, which was not to present current projects but instead, to bring together the wider and global trust and security communities to explore how best to organise future International cooperation (INCO) research activities and its supporting programmes, together with the identification of the key challenges, issues and priorities to tackle together. Mr. Clarke explained how the agenda was formed in order to cover the core objectives of the Annual Forum.

Objective 1. *Identification of the technological challenges that really need and could be tackled in common between the countries so they can be elaborated clearly with the policy makers in the respective countries as a way forward;*

This objective was being covered by a presentation on Identification of advantages for international cooperation and the trust and security technological challenges – BIC review of research topics already identified; and panel session 2. Human oriented approaches to security, privacy and trust and how international cooperation can benefit; and panel session 3. Digital ecosystems network and information security and how international cooperation can provide mutual benefits.

Objective 2. *Highlighting the current bi-lateral (and potentially overlapping) country to country cooperation(s) into a more comprehensive unified global cooperation;*

This objective was being covered by the opening session on Setting the scene with DG INFSO views on International Cooperation and Panel session 1. Other INCO-related projects with direct or indirect linkages to ICT trust and security aspects.

Objective 3. *From the insights of the researchers and programme managers, to explore how best to organise future International cooperation (INCO) research activities and its supporting programmes, together with the key challenges, issues and priorities.*

This objective was being covered by Panel session 1. Other INCO-related projects with direct or indirect linkages to ICT trust and security aspects; and panel session 2. Human oriented approaches to security, privacy and trust and how international cooperation can benefit; and panel session and 3. Digital ecosystems network and information security and how international cooperation can provide mutual benefits; and the closing session on planning and operations.

Setting the scene with European Commission DG-INFSO views on INCO

International cooperation in the ICT theme of the FP7 programme – Alvis Ancans

Speaker: Alvis Ancans is in the Information Society and Media Directorate General (DG INFSO) of the European Commission. He is an International relations officer within the Unit A2, International Relations.

Alvis Ancans outlined his talk, which would focus on international cooperation in the ICT theme in the FP7 programme in which there is currently a strong emphasis on international cooperation.

In the FP7 research programme, it operates on a basis of calls for proposals in which proposals are submitted to address these and the next call (number 8) has a deadline of 17th January 2012. The following table highlights the objectives currently open.

Challenge	Objectives for Call 8 (deadline 17 January 2012)
Challenge 1: Pervasive and Trusted Network and Service Infrastructures	ICT 2011.1.1 Future Networks ICT 2011.1.2 Cloud Computing, Internet of Services and Advanced Software Engineering ICT 2011.1.4 Trustworthy ICT ICT 20011.1.6 Future Internet Research and Experimentation (FIRE)
Challenge 3: Alternative Paths to Components and Systems	ICT 2011.3.1 Very Advanced NanoelectronicComponents: Design, Engineering, Technology and Manufacturability ICT 2011.3.2 Smart Components and Smart Systems Integration ICT 2011.3.5 Core and Disruptive Photonic Technologies
Challenge 4: Technologies for Digital Content and Languages	ICT 2011.4.4 Intelligent Information Management
Challenge 6: ICT for a Low Carbon Economy	ICT 2011.6.1 Smart Energy Grids ICT 2011.6.3 ICT for Efficient water Resources Management ICT 2011.6.7 Cooperative Systems for Energy Efficient and Sustainable Mobility
Challenge 8: ICT for Learning and Access to Cultural Resources	ICT 2011.8.1 Technology-Enhanced Learning
Future and Emerging Technologies	ICT 2011.9.6 FET Proactive: Unconventional Computation (UCOMP) ICT 2011.9.7 FET Proactive: Dynamics of Multi-Level Complex Systems ICT 2011.9.8 FET Proactive: Minimising Energy Consumption of Computing to the Limit (MINECC) ICT 2011.9.12 Coordinating Communities, Identifying New Research Topics for FET Proactive Initiatives… ICT 2011.9.14 Science of Global Systems
Horizontal Actions	ICT 2011.11.1 Pre-Commercial Procurement Actions

The next Call 9 will open in January 2012 and close in April 2012. There will be a specific objective on international cooperation ICT 2011.10.3 called International Partnership Building and Support to Dialogues (Enable Partnership Building in Low and Middle Income Countries, incl. Africa)

The Commission recognises the need to cooperate internationally, with the following objectives:

- To jointly develop ICT solutions to major global societal challenges;
- To jointly respond to major global technological challenges by developing interoperable solutions and standards;
- To improve scientific and technological cooperation for mutual benefit.

A number of general points were raised about the supports related to international cooperation, including international partners welcome in all Challenges and Objectives and there is an eligibility criteria that needs to be satisfied including a minimum of 3 different EU Member States or Associated Countries and beyond this minimum, all non-EU/non-AC countries can participate. For targeted openings in which countries are specifically mentioned within the objectives, the participation of third countries is particularly encouraged. There have been some horizontal actions on international cooperation including coordinated calls with Brazil and with Russia and related to international partnership building and support to dialogues. A number of past, current and future targeted open calls were highlighted on a country by country basis.

Japan

Calls 7, call 8 and call 9 had targeted calls with Japan in the following objectives:

Call 7: deadline passed

- Objective ICT-2011.1.3 Internet-connected Objects,
- Objective ICT-2011.3.6 Flexible, Organic and Large Electronics and Photonics.
- Objective ICT-2011.5.2 Virtual Physiological Human

Call 8: deadline 17 January 2012

- Objective ICT-2011.1.1 Future Networks,
- Objective ICT-2011.1.2 Cloud Computing, Internet of Services and Advanced Software Engineering,
- Objective ICT-2011.3.1 Very Advanced Nanoelectronic Components,
- Objective ICT-2011 9.6 FET Proactive: Unconventional Computation (UCOMP).

Call 9: deadline April 2012

- Objective ICT-2011.5.2 Virtual Physiological Human

Brazil

There already was a first EU-Brazil coordinated call announced in September 2010 at the ICT 2010 event, Digitally Driven with a joint funding of €10 million (€5 million each side). After evaluation and negotiation, five projects started in May-Sept 2011 with average project durations of 24-30 months. The projects being funded are in the areas of Future Internet Experimental Facilities and Security, Microelectronics and Micro-Systems, Networked Monitoring and Control, and e-Infrastructures. In November 2011, an agreement was reached between the European Commission and the Brazilian government to launch a new EU-Brazil coordinated call with a joint

funding of €10 million. The Call for Proposals will focus on such areas as cloud computing for science, sustainable technologies for smart cities, smart platforms for a smarter society, and hybrid broadcast-broadband TV applications and services. Following evaluation and negotiation, projects are expected to kick-off in 2013.

Russia

The first coordinated call under the FP7 ICT 2011-2012 Work Programme was agreed with the Russian Ministry of Education and Science. The focus was on the following areas: Programming Models and Runtime Support, Performance Analysis Tools for High-Performance Computing Optimisation, Scalability and Porting of Codes. As a result, two EU-Russian coordinated projects started in Feb 2011. Both are separate EU and Russian projects linked through a coordination agreement: 1. HOPSA (HOlistic Performance System Analysis); duration 24 months; funding: €1.4 million from the EU side and 20 million roubles from the Russian side; 2. APOS (Application Performance Optimisation and Scalability); duration 24 months; funding: €1.2 million from the EU side and 19 million roubles from the Russian side.

What does the future hold for International Cooperation?

The work programme for 2013 is currently under preparation and is expected to be published in the first half of 2012. It is expected that there will be coordinated Calls with Brazil and Russia (currently under discussion; topics: high-performance computing and semantic web) and the possibility of coordinated Calls with Australia, South Africa, Mexico and Japan are in the pipeline – more likely in 2013. On the international cooperation theme (CSA), there is an expected budget increase (up to €7 million) and a comprehensive geographic coverage.

On the question of who can participate:

- Three independent legal entities from three different EU Member States or Associated countries (presently: Albania (AL), Bosnia-Herzegovina (BA), Croatia (HR), the Faroes (FO), Iceland (IS), Israel (IL), Liechtenstein (LI), FYR of Macedonia (MK), Montenegro (ME), Norway (NO), Serbia (SR), Switzerland (CH), Turkey (TR));
- EEIGs composed of members that meet the criteria above can participate;
- International (intergovernmental) organisations;
- participants from third countries **if in addition to minima;**
- Collaborative projects for specific cooperation actions (SICA) dedicated to international cooperation partner countries (ICPC): minimum 4 participants of which 2 in different MS or AC and 2 in different ICPC countries unless otherwise specified ;
- Support actions; no restrictions.

The talk concluded with a summary of the eligibility for community funding:

- Legal entities from MS and AC or created under Community law (and the JRC);
- International European interest organisations;
- Legal entities established in international cooperation partner countries (ICPC-INCO);
- Legal entities established in 3rd countries other than ICPC-INCO, if provided for in SP or WP; or if essential for carrying out action; or if funding is provided for in a bilateral agreement between Community and that country.

Panel Session 1. Other INCO-Related projects with direct or indirect linkages to ICT trust and security

EU-India Spirit project[16] – Tom Williamson

Speaker: Tom Williamson (TW), European Research Consortium for Informatics and Mathematics, European Economic Interest Grouping) ERCIM EEIG. He is the project co-Ordinator of Euro-India SPIRIT project.

1. *How does your project contribute to International cooperation and trust and security?*

The EU – India Spirit project seeks to build consensus between the EU and India on areas of collaborative research across the ICT spectrum and the area of trust and security is a central part of its work. We're in the process of producing a final set of recommendations with some targeted areas of suggested international cooperation in this area; including but not limited to: usable security in the mobile world, large scale data security and ID management.

2. What are the benefits and expected impact of your project brought on by international cooperation?

From the EU – India Spirit project perspective, obviously it's our hope that the recommendations produced will be further taken up and implemented by the respective governments, difficulties in finalising arrangements for a Joint Working Group (JWG) notwithstanding. In terms of the benefits accruing to the partners as a result of participation in an international cooperation action, the Indian partners have increased visibility and familiarity with Commission-funded projects, in particular, and EC processes in general as well as strong relationships with consortium members and related entities. Both sets of partners obviously benefited enormously from cross-cultural experiences in terms of travel, working norms and approaches to networking over the course of the project.

3. International cooperation is not an easy task and required a lot of patience and time. What are the issues encountered and how did you address them?

Issues can be wide-ranging. Difficulties in scheduling face-to-face meetings are obviously magnified in international cooperation projects with such significant scale to contend with and as a coordinator, it's very important that you find ways to work around this through regular teleconferences etc. Time and distance are factors in terms of travel and events require careful scheduling further in advance. Especially in the model of project that I'm involved in, where you need the time not only of your consortium members but also external experts, significant advance notice is required.

[16] http://www.euroindia-ict.org/

4. In the opening session, it was mentioned by the Commission that INCO projects should go further than just identifying stakeholders and who the counterparts are in the countries and topics of cooperation. What are your projects plans to take this approach for a longer term strategy and is there anything that BIC can do to help you with this strategy.

The EU – India Spirit project is finishing at the end of December 2012 so it is difficult to plan a longer term strategy beyond this and it hasn't been built into the legacy planning. In terms of BIC, it is highly recommended to continue the collaboration in the countries and it has been a highly mutual benefit to have a number of the BIC members involved in the working groups of EU – India Spirit from the very start.

5. What are your recommendations for improving effectiveness?

The day to day working of the SPIRIT project has not been as radically different from exclusively EU-based projects as might have been initially expected. I would say that in terms of improving effectiveness, greater emphasis should be placed on widening the net of participating international partners, so as to ensure that consortia are to the greatest extent possible comprised of partners with the most appropriate competencies and not the limited pool of potential partners who are already familiar with the FP7 structure and have previously participated in projects. In this regard, projects promoting international cooperation such as BIC, India-Gate and its equivalents for the other BRIC countries are crucially important.

Synchroniser project[17] – Katja Legiša

Speaker: Katja Legiša is an Italian consultant with seven years of experience in international and EU project management, promotion and support of research and development activities. Her professional and educational background is in Project Management, Public Relations and Communication. Since 2006 she is coordinating EU-India projects. She is now the Project Coordinator of the SYNCRONISER project.

1. *How does your project contribute to International cooperation and trust and security?*

Synchroniser boosts the impact of the policy dialogue by identifying EU-India research priority areas and recommendations on how to improve the cooperation. The identified areas, the recommendations together with the action plan is then delivered to the DIT (India's Department of Information Technology) and EC. The method used by the project is to organize policy dialogue meetings with high level EU – India experts and a foresight exercise on medium and long term research trends and perspectives: Delphi study on technology priorities in ICT R&D identified by thirty visionaries of India. The study aim at understanding what India might prefer to invest in, in ICT R&D in the next 2, 5, 10 years. One of the identified research priorities is also *Security, Privacy & Monitoring* (data management system, secure storage system, person identification and tracking systems; for healthcare, governance and education).

2. What are the benefits and expected impact of your project brought on by international cooperation?

The Joint Working Group (JWG) on ICT was established in 2004 between European Union and the Government of India's Department of Information Technology (DIT). The JWG is mainly comprised of policy-makers and concerned ministers from both regions including very few researchers and stakeholders. The JWG meetings are inter-governmental, closed-door meetings which follow a top-down approach. In this scenario, actors from the two regions never meet in a common platform to discuss JOINT research Priorities. SYNCHRONISER aims to fill this gap by bringing together the 'gurus' of the research and stakeholder communities of both regions on a common platform as "analyzers of these Joint research priority areas", thus providing a more **practical, consultation approach** to boost the impact of policy dialogues on Joint research priority areas, Synchroniser uses a **bottom up approach** in which the project provides the EC with the evidence, on which they can make policy decisions.

3. International cooperation is not an easy task and required a lot of patience and time. What are the issues encountered and how did you address them?

The difference of viewing time and deadlines is different between the two countries, which brings to difficulties in carrying out joint activities. Time can be

[17] http://euroindiaresearch.org/synchroniser/

viewed in the form of a line or in the form of a circle: For Indians: a beginning is not the beginning and the end the end, but a continual cycle of beginnings and endings. The past, present and future, are circular, interconnected, that is why time is less important. The arrow of the timeline gives irreversible processes; it has a start and an end. The past present and future are not necessary connected. The difference between Formal and Informal communications plays an important role in getting things done and especially when passing a message across.

4. In the opening session, it was mentioned by the Commission that INCO projects should go further than just identifying stakeholders and who the counterparts are in the countries and topics of cooperation. What are your projects plans to take this approach for a longer term strategy and is there anything that BIC can do to help you with this strategy.

Both the EU – India Spirit and Synchroniser projects have had long term planning problems due to the periodic postponements over the last 2 years of the main DIT/EU meeting. However, this same situation resulted in this very topic of long term planning to be included as a key recommendation being made by the project. For liaising with other projects like BIC, this is also included in a recommendation that the follow up work can be directly or indirectly supported by other projects and/or other initiatives or channels. As part of the recommendations, an action group is being proposed to continue after the project. In addition, it should be noted that the Synchroniser project are not just trying to find the research topics for collaboration but it is also concentrating on recommendations on how to improve the longer term cooperation between the countries e.g. via other means apart from the projects something that could stay in place for a longer period of time. Some examples in discussions include: Executive bodies, collaboration with EU based eTPs, forming India based eTPs, which would be discussed in more detail later. This approach came up as the project recognises that research priorities have a strong tendency to change from year to year and we need something more everlasting. This is what is missing now and needs to be addressed as a matter of urgency.

5. What are your recommendations for improving effectiveness?

Recommendations include setting up **collaboration with ETPs and xETP Initiatives** in order to launch the Indian Technology Platform Channel. This tool would be horizontal to All ICT related ETPs in order to bring the Indian flavor to the debates within the ETPs and the xETP Innovation initiative. It is also recommended to **involve Indian experts in the ISTAG** related activities: Search on the mechanism which would allow Indian experts to get involved in the relevant bodies shaping priorities and strategic directions of the FP7/Horizon 2020. Another recommendation is to establish a JWG Action Group for executing JWG outcome: Proposal to establish a JWG **Action Group** that could execute the JWG outcome. The form could be flexible (nomination of officers by EU and India, Support Project, Tenders, ...). The Action Group would be a sort of executive office to undertake the decisions adopted by the JWG. Another recommendation is a proposition of **a Co-funding Model** for DIT: *Analyse Energy and Biotechnology co-funding programmes (between EC & DST).*

EURASIAPAC project[18] – Fernando Kraus Sanchez

Speaker: Fernando Kraus Sanchez, Director of the Foreign Affairs Sector within the Research and Innovation division of AToS in Spain. Fernando has over fifteen years of experience in participating in the implementation of ICT projects including the EURASIAPAC project. He has wide experience in the field of exploitation and marketing activities as a senior consultant both in the private and public sectors of different countries (Argentina, Azerbaijan, Brazil, Cameroun, Dominican Republic, Egypt, ..). Additionally, he has been highly involved in the management of European and National R&D projects (Cockpit, ImmigrationPolicy2.0...) as well as in managing multi-people teams.

1. *How does your project contribute to International cooperation and trust and security?*

Eurasiapac focuses on ICT research cooperation between the EC and the Asia-Pacific region, mainly Korea, Japan, Australia and New Zealand.. Eurasiapac has provided a global picture of themes of interest in ICT, priorities, tendencies, difficulties in cooperation, reasons why to search cooperation, sources of information used in each country.

a. European and Asian-Pacific institutions declared strong interest in pursuing cooperation/collaborative research with each other and share the main motive to seek cooperation and research: "*knowledge (technology) exchange*". A high number of EU respondent organizations recognize searching cooperation as a mean to market penetration and development in the AP region, reason which is not so relevant for AP respondents.

b. No clear thematic focus for cooperation was cited by EU respondents while Future and Emerging Technologies is a dominant focus for AP countries. EU respondents expressed interest in Future and Emerging Technologies at similar level to "ICT for Mobility, Environmental Substantiality and Energy Efficiency", "ICT for health and wellbeing" and "ICT for learning and access to cultural resources". Other thematic priorities for AP respondents are 'ICT for mobility, environmental substantiality and energy efficiency', "Cognitive Systems, Interaction, Robotics" and 'ICT for health and wellbeing'.

c. By countries, EU respondents has cooperated mainly with Japan and Korea and, to a slightly lesser extent, with Singapore, Taiwan, Australia and New Zealand, by this ranking. The EU countries to cooperate with for AP respondents are the UK, Germany, France, Netherland and Sweden. Over half of respondents are interested in cooperating with Spain.

Eurasiapac has enabled the creation of links between ICT researchers between the mentioned countries through workshops carried out in each countries and constant cooperation during the last 2 years.

Trust and Security has been identified as one of the priorities among the topic of interest in ICT research in the countries participating in the project.

[18] http://eurasiapac-fp7.eu/

2. What are the benefits and expected impact of your project brought on by international cooperation?

Through the surveys carried out among the researchers community, we have identified joint common topics of interest in ICT research between EC and Korea, Japan, Australia and New Zealand.

The contacts and the fact that some main stakeholders in ICT research have been directly involved in the project – consortium partners are CSIRO in Australia, KIAT in Korea, Fraunhofer Japan, University of Canterbury in New Zealand , and Fraunhofer, Atos and Sigma in the EC - has raised interest in launching joint call with some of the countries. Joint calls with Japan and Australia are under preparation and are expected to be launched in 2012 or 2013.

3. International cooperation is not an easy task and required a lot of patience and time. What are the issues encountered and how did you address them?

Although the Eurasiapac project focuses on ICT cooperation between EC and the Asia-Pacific region, it's difficult to deal it as a homogeneous region because each participating AP country (Japan, Korea, Australia, New Zealand) has different characteristics, institutions and approach to ICT research, i.e. they are not homogeneous. In Europe, the EC FP7 creates a common approach to research, but it doesn't exist a similar common institutions in the Eurasiapac targeted countries. Each country needs to be dealt in a different way

On a day-to-day cooperation, the fact that there are 10-12 hours of time differences between the countries difficult the usual working cooperation process. A call conference among all partners always causes a "sacrifice" for one or another partner, as it can't be held at a standard working daily time for all partners.

IPR is always an issue in international ICT research cooperation and needs to be dealt at a very early stage of the research process.

4. In the opening session, it was mentioned by the Commission that INCO projects should go further than just identifying stakeholders and who the counterparts are in the countries and topics of cooperation. What are your projects plans to take this approach for a longer term strategy and is there anything that BIC can do to help you with this strategy.

This is an issue that was highlighted and attempted by EURASIAPAC also but it was found to be incredibly difficult as even though the project's overall goal was to consider the cooperation between the EU and the entire ASIAPAC region as a whole, in actual fact, there are considerable differences between the countries involved and these always need to be factored into the discussions and cooperation models. Therefore, a bi-lateral approach is absolutely necessary even if there are some common cooperation issues across the regions.

5. What are your recommendations for improving effectiveness?

Joint calls are already being prepared with Australia and Japan. A Japan – EU S&T Cooperation agreement has entered into force on 29 March 2011, aiming at promoting a structured S&T policy dialogue between Japan and the EU. We need to crreate more agile processes to define, launch and approve ICT cooperation initiatives. Many of the Asia-Pacific institutions involved in the projects, mentioned that the period of time to create, prepare and launch a cooperation initiative should be shorter as the view is that EC processes take too long. Understanding legal and administrative EC funding processes are not always easy for non EC institutions; simplified methods may enhance international participation.

SECFUNET project – Marcelo Pasin

> **Speaker: Marcelo Pasin**, Assistant professor at the University of Lisbon. Previously, he was a researcher at INRIA (France, 2007-2008) and tenured associate professor at the Federal University of Santa Maria (Brazil, 1991-2007). He has worked for CoreGRID, EGEE and EC-GIN in FP6, and is now working for TClouds and SECFUNET in FP7. SECFUNET is a project from within the recent EU-Brazil joint call held during Call 7 of FP7.

1. How does your project contribute to International cooperation and trust and security?

SECFUNET is a STREP in FP7, with EU and Brazilian partners. It proposes to create a new generation in the Internet security that is very simple to use (no need of a specialized skill). It is based on secure microcontrollers, has strong authentication with privacy and secure identity management. It is intended for use with virtual networks and clouds, offering isolation, reliability and encryption.

2. *What are the benefits and expected impact of your project brought on by international cooperation?*

SECFUNET's partners are very heterogeneous: Brazilian and European partners complement each other. We have a large number of partners, with many different skills. It would be hard to gather these skills without cooperation. Specifically from Brazil we get different perspectives, very different regulation frameworks and very different concerns. Brazilians also include a pioneer researcher in intrusion-tolerance and a national networking research laboratory. SECFUNET also allows for leveraging previous cooperation, that would otherwise be impossible.

3. *International cooperation is not an easy task and required a lot of patience and time. What are the issues encountered and how did you address them?*

In time scales, the start times were very different and this caused a lot of problems. EU – started May and Brazil are only now hiring as they received funding in October. So EU partners started long before.

Cooperation projects in Brazil are not structurally the same as in EU. They are not used to the types of joint projects, which include meetings, discussions, workshops, etc. They are just used to meeting at the beginning and then work on the project in an independent fashion. It will take a while for them to get used to it. The evaluation process is also very different between EU and Brazil. In Brazil, reporting is carried out mainly in the very end of the project, therefore, making it difficult to get things going in terms of a common progress reporting mechanism between the countries. Another example is Brazilians are not responsible for delivering to the EC. These efforts need to be harmonised between the participants in the different countries.

4. *In the opening session, it was mentioned by the Commission that INCO projects should go further than just identifying stakeholders and who the counterparts are in the countries and topics of cooperation. What are your projects plans to take this approach for a longer term strategy and is there anything that BIC can do to help you with this strategy.*

As a perspective for longer term exploitation, we have several industrial partners. We feel it is the combination of the companies that are going to do their development of their products within the projects in order for the project to have a longer term impact for both the partners and the project in general. Twinteq wants to develop its products in near-field communication, EtherTrust and Implementa work with secure elements like SIM cards, and Infineon wants to boost its trusted components for the future networks. More generally, SECFUNET wants to establish a sound security infrastructure that could be used by anyone.

5. *What are your recommendations for improving effectiveness?*

As recommendations for improving effectiveness, I suggest better agreements with non-European authorities, with, for instance, better definitions in the commitments, and better synchronisation. It could include previous negotiation for project management standards, as, for example, how to deal with deliverables, project review and evaluation. The European Commission should help the targeted applicants to have knowledge of its rules and evaluation standards, using, for example, concertation meetings in the targeted countries.

FEAST/FEED/AUS-ACCESS4EU/SECAS/ projects – Rado Faletic

Rado Faletič (RF), Executive Director of FEAST. Rado's involvement with the *Forum for European-Australian Science and Technology cooperation* (FEAST)[19] stems from his interest in promoting, encouraging and highlighting science and new ideas, along with the personal satisfaction he receives from facilitating individual collaborations. He has previously held a number of research, teaching and IT positions at The Australian National University, including appointments at the Research School of Chemistry, the Research School of Earth Sciences, the Research School of Humanities, the Research School of Social Sciences and the Australian National Institute for Public Policy. At ANU, Rado has also completed a PhD in shock tunnel tomography (rocket science!). His other research projects have included the spatial modelling of water flow in de-forested landscapes, and seismic tomography.

1. *How does your project contribute to International cooperation and trust and security?*

Within the panel, Rado Faletič represented a number of projects.

FEED (www.feast.org) The *FEAST Extension, Enhancement and Demonstration project* (FEED) project is the third iteration of the BILAT with Australia (2008-2012). The explicit objective of the BILAT projects is to highlight and facilitate R&D collaboration between Europe and the target third countries (in this case… Australia). We operate a support helpdesk for all research fields, act as NCP's for Australia, and provide information and support to the government-government JSTCC meeting between the EU and Australia. The ICT meeting as a part of the most recent JSTCC (in 2010) identified trust and security as a priority area of collaboration between Europe and Australia. We have conducted bibliometric studies on EU-Australian collaborations, though there is a poor coverage of ICT publications. We also conducted an extensive stocktake of Australian involvement in FP7.

AUS-ACCESS4EU (www.aus-access4.eu) *Supporting EU Access to Australian Research Programmes* (AUS-ACCESS4EU) catalogues and promotes Australian funding opportunities available to European researchers, and conducts studies on Australian research strengths and the openness of Australia's funding programmes.

SECAS (www.secas.eu) *Strategies for European ICT RTD Collaboration for Australia and Singapore* (SECAS) is a sister project to EURASIAPAC. It identified ICT thematic capabilities and areas of potential synergy, performed policy analysis and has made strategic recommendations for improved cooperation policies. This project performed the first lab-level systematic analysis of ICT research groups in Australia, thematic strengths etc, which has delivered results that are now ready to be used. Trust and security topics are clearly identified in the final report, which is now available online.

2. *What are the benefits and expected impact of your project brought on by international cooperation?*

Both FEED and AUS-ACCESS4EU have greatly contributed to the flow of information between Europe and Australia regarding overall funding modalities available for international collaboration, but more importantly have identified and developed strategies on how to most successfully use these mechanisms (including

[19] http://www.feast.org/

FP7, COST[20], ARC[21] and NHMRC[22]). SECAS has produced a concrete set of strategic recommendations, which are available in the final public report online.

3. *International cooperation is not an easy task and required a lot of patience and time. What are the issues encountered and how did you address them?*

One of the issues of most importance has been the persistent lack of understanding, particularly in Europe, regarding how to include third country partners on FP7 proposals. FEED and AUS-ACCESS4EU have been working actively (through email alerts, but more affectively through targeted seminars and direct communication) to education both Australian and European researchers on *the facts* as well as *the realities* of including Australian partners on FP7 projects. This includes issues of funding support. SECAS has identified issues ranging from abstract political ones (e.g. that policies need to be concrete, should also include technical content, and need follow-up actions) to practical ones at the researcher level (e.g. how to best work over long distances, the benefits of setting up joint labs, the challenges of researcher exchange, etc.).

4. *In the opening session, it was mentioned by the Commission that INCO projects should go further than just identifying stakeholders and who the counterparts are in the countries and topics of cooperation. What are your projects plans to take this approach for a longer term strategy and is there anything that BIC can do to help you with this strategy.*

The issue of sustainability has been a very important one especially within the FEED/BILAT projects where they have started working already with what they call 'multipliers' to impart their knowledge and key ideas around Australia. For other projects, it is an issue. What can projects do during their lifetime so the work can continue? BIC can talk to the SECAS project to see if there is anything BIC can do to help create this value.

The BILAT project, one of which just finished are putting together significant workshops on specific topics. BIC can help develop the content and identify the individuals who can contribute to this workshop. This can lead to more lasting co-operations.

5. *What are your recommendations for improving effectiveness?*

We have noticed a lack of coordination and information-sharing between the variety of INCO activities across FP7. We propose that consideration be given to this issue in future INCO calls, and recommend that activities be developed to facilitate the integration of activities amongst all INCO projects, particularly so that findings can be directly implemented into ongoing projects (rather than waiting for final reports, which in any case are rarely read by other INCO actors).

[20] http://www.cost.eu/
[21] http://www.arc.gov.au/
[22] http://www.nhmrc.gov.au/

Keynote: Identification of advantages for international cooperation and the trust and security technological challenges – BIC review of research topics already identified – Michel Riguidel

Speaker: Michel Riguidel is Professor Emeritus, 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 is contributing to the Coordinated Action in international security research of the FP7 BIC (2011-2013) and caretaker for security and trust of the FIA (Future Internet Assembly). He has several patents in security (firewall, watermarking and protecting CD ROM, illicit content downloading).

In starting out his talk, Michel Riguidel explained in some detail the shifts in paradigms that we are encountering where it is increasingly difficult to attain a trusted and secure global digital communication and information handling system via a dependable international ICT infrastructure. This will continue to be based on an evolving Internet, together with the many services that rely on it to deliver their benefits. Many of these services are now integral parts of our daily lives and the fabric of our societies, and are increasingly part of our cultures. However, the whole edifice – Internet and Services – is currently quite frail and vulnerable to both attack and failure. The remedies include repair, shoring up and reinforcement, and eventual replacement over time by more modern robust or resilient designs and components.

A general recommendation made by Professor Riguidel is that it is essential to continue current initiatives and the ongoing consensus towards our goal of increasing the trustworthiness, dependability, and security of interoperable global ICT. Through the BiC project – Building International Cooperation for Trustworthy ICT: Security, Privacy and Trust in Global Networks & Services and previously INCO-Trust as explained in the opening talks, work is already in progress that will maintain, and indeed extend, the dialogue between Europe and international partners in pursuance of our goal. Through these projects, we are engaged in identifying topics and themes recommended for further elaboration leading to international collaboration and cooperation leading towards a stronger, more trustworthy global communications – where this inevitably involves the Future Internet.

Within the INCO-Trust project, a number of recommendations were made within their final deliverable D3.1 INCO-Trust Final recommendations **report**[23]. Two groups of recommendations are Strategic and Tactical and these were presented in brief by Prof. Riguidel. It was pointed out that the ordering of the recommendations is not meant to imply any over-riding chronological order, but that the Strategic group are meant to be the pre-requisite enablers for international cooperation, setting out the frameworks, common understandings and motivations, and overall landscape to ensure the possibility and effectiveness of the more concrete Tactical group recommendations.

[23] http://www.inco-trust.eu/media/D3_1_report.pdf

The recommendations made here are split into two groups:

- Strategic: setting out the frameworks, common understandings, and overall procedural and governance landscape that takes into account the diversity of social, economic, and cultural norms and requirements worldwide;
- Tactical: research towards the technical building blocks and their relationships that will enable a trustworthy, secure ICT ecosystem.

(a) Strategic Recommendations

SR1 **International alignment**: preparation of policy frameworks to enable global collaboration and interoperability

SR2 **Variety**: cooperation on topics related to security and diversity.

SR3 **Scalability**: cooperation on topics related to security and complexity

SR4 **Reciprocity**: cooperation on topics related to security and interoperability

SR5 **Secrecy**: cooperation on the issues of digital sovereignty and dignity

SR6 **Negotiation**: cooperation on the theme of security and trust

SR7 **Security expertise**: cooperation on topics related to security and technological challenges of security

SR8 **Protection:** cooperation on topics related to security and cyber-defence

(b) Tactical Recommendations

The international ICT trust and security community should collaborate on research to:

TR1 Support strengthening infrastructure resilience and control crisis management.

TR2 Support securing the current and future Internet related to diversity, complexity and interoperability.

TR3 Support securing cloud computing for enterprises.

TR4 Support designing identity and accountability management frameworks.

TR5 Support new privacy infrastructure, reconsidering privacy spaces, storage function areas.

TR6 Support repositioning trust infrastructure at the same level as security infrastructure.

TR7 Support metrics and standardization issues.

TR8 Initiate green security.

TR9 Support cooperation in cyber-defence against the asymmetric challenge

TR10 Enable the engineering of secure and trustworthy software and systems.

Professor Riguidel summarised the four main themes that have been highlighted in the project's bi-lateral cooperation events to date. These include:

Theme 1: Digital ecosystem security (Network & Information security) oriented to the System. This theme involves protection and trustworthiness with the strengthening of infrastructure resilience and control crisis management, crisis management (CIP), Security and cyber-defence (incl. against the asymmetric challenge). It also includes securing the current and Future Internet, network/system security, securing cloud computing for enterprises, Mobile security, security for mobile connectivity. In addition, it deals with policy properties such as variety, scalability, reciprocity, diversity, complexity and interoperability.

Theme 2: Trust & Privacy (including personal data protection) oriented to the Humans, Users. It incorporates topics related to responsibility (Identity versus Anonymity), designing identity and accountability management frameworks, international Privacy friendly authentication and reputation assurance. It includes measurement and negotiation, repositioning trust infrastructure at the same level as security infrastructure and trust management. Other areas under this theme include secrecy, dignity, sovereignty designing digital sovereignty and dignity, and new privacy infrastructures, reconsidering privacy spaces, storage function areas; and, last but not least, usability creating a Human oriented and usable security for citizens.

Theme 3: Global Framework & International alignment oriented to principles & governance. This includes properties such as interoperability, openness, transparency and secrecy; the preparation of policy frameworks to enable global collaboration and interoperability; Knowledge and International Data exchange architectures for cybersecurity; and socio-economic aspects including data policy, governance and secure, trustworthy and viable ecosystems.

Theme 4: Methodology, tools and technical challenges oriented to the tools. Under this theme is expertise sharing in science, technology & engineering; methods to support metrics and standardization issues; software security to enable the engineering of secure and trustworthy software and systems; protection of data and information with cryptology (digital signature, etc.) and other upstream topics including the initiation of green security.

In conclusion, Professor Riguidel presented a table showing a summary of all of the countries interactions to date, showing the programme /funding agency contacts, research level contacts and a sampling of the priority research themes for international cooperation in trust and security. The full table can be found on the next page.

Table 1. Summary of all of the countries interactions to date

Country	Program Level	Research level	Priority research themes for INCO
USA	National Science Foundation Department of Homeland Security	Massachusetts Institute of Technology, Rutgers University, University of California, San Diego, University of California, Davis, University of Illinois , Others	CyberSecurity/Privacy: Technology and Usage Issues Trustworthy International information exchange including data transfer and sharing, Security models for the Future Internet.
Canada	National Science & Eng. Res. Council	Univ. of New Brunswick, Ecole Polytechnique Montreal	Industry driven projects on trust, security and privacy.
Korea	Ministry of Knowledge Economy, KEIT	SoonChunHyang University, Seoul National Univ. Others	Internationalisation of data (identity management, privacy, end to end trust metrics, ...); Countermeasures against Massive DDoS; Security of Cloud computing e.g. Security of Smart Grid; Security compliance management and information security assurance; Security for VoIP and Mobile communications; Future Internet.
Japan	Japan Science and Technology Agency, CREST programme, MIC	NICT, University of Tokyo, Tokyo Inst. of Tech, JAIST, Others	Dependability, Security, Privacy and Trust of embedded systems
Australia	Australian Research Council (ARC)	CSIRO, NICTA, Macquarie University, Univ. of Sydney, IIS Partners, many others	Communications Security, Trust and Privacy in the Future Internet; Formal approaches for trust and security.; Sensor networks.
Brazil	CNPq (National Research council), FUNTEL, State Research foundations ITI (Instituto Nacional de Tecnologia da Informação)	Universidad de Brasilia, Univ. of Sao Paulo, CPqD Serasa Experian, Others TBD	Future Internet, Wireless Technologies: Security, Privacy, Trust over ad-hoc networks, Quantum crypto, ID management.
South Africa	SA Dept. of Science and Technology SA Technological Innovation Agency	Council for Scientific and Industrial Research (CSIR) – The Meraka Institute, SAP, University of Pretoria, University of Johannesburg, University of South Africa, others	Wireless Technologies: Security E-infrastructures security and trust
India	Dept. of Information Technology (DIT), ERNET, EuroSpirit India Support action (FP7)	India Institutes of Technology (IITs), India Institute of Science (IISc), Universities - Hyderabad, Pune, Anna amongst others).	Data Center Security, Data Privacy, ID card, ID management.

Panel Session 2. Human-oriented approaches to security, privacy and trust and Chair: Priscila Solis Barretto

Human-oriented and Usable Security – Karima Boudaoud

Speaker: 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 serverd 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

With the growth of Internet, one of the most sensitive issues of our "always connected" society is the security of electronic data. The issue concerns everyone: individuals, corporations and public institutions. At the Network and Information Security Management: research ideas workshop [24] held on 22nd September 2011, one of the main recommendations was there is a need to examine human oriented security solutions as the generation of users is changing as they are born and raised with ICT and studies show they would be more open to use security solutions and the security designers need to listen and adapt their solutions according. At the workshop, there were discussions about the level of evidence about young people caring more about security and privacy. There is mainly anecdotal evidence on this that while some users will ignore these issues, there are considerable levels of users that care about their security and privacy. It was agreed that researchers should not take as a starting point that young people don't care about security and privacy. Instead, all of the points of view should be studied from the sociological perspectives and involve the right stakeholders in our research projects.

Security management should be more accessible to all kind of users and especially non-security experts evolving towards a more human oriented security management vision. To address today's security issues, we need to: 1) move from the traditional technology-only oriented design of security solutions towards user-centric security management and 2) bring together experts from psychology, social science, economics, legal, technologists and security experts to address security and privacy from a user point of view and put her/him at the heart of problem.

From an international point of view, we need:

- Collaboration between security experts and experts from other disciplines (psychology, social science, etc.) and from different countries, in addition to collaboration with international government institutions.
- Organisation of **multidisciplinary** and **international workshops** targeting wide public.
- Set up of **multidisciplinary** and **international working groups** in targeted countries.
- Collaboration with standardization organisations.

[24] http://cordis.europa.eu/fp7/ict/security/events_en.html

Privacy-respecting Authentication – Ioannis Krontiris

Speaker: Ioannis Krontiris, is a senior researcher in the group of Mobile Business and Multilateral Security at **Goethe University Frankfurt**. Ioannis holds a PhD from Mannheim University, Germany and a MSc degree from Carnegie Mellon University, USA. He is currently involved in the coordination of the EU-Project ABC4Trust (Attribute-based Credentials for Trust) where he is also leading the architecture work package. His main research interests include Identity Management, Online Privacy, Security and Privacy in Pervasive Environments.

Europe aims for an electronic identity management infrastructure as a basis for trustworthy services in e-government and e-commerce to overcome fragmentation, closed solutions and lack of user control and transparency. The outcome of the EU-project ABC4Trust will result in important input for the design of the upcoming electronic identity management infrastructure, by closing the gap between the architectural framework level and the crypto level that slows down the adoption of privacy respecting attribute-based credentials systems (Privacy-ABCs), as well as making the infrastructure independent of specific implementations.

Towards this goal, ABC4Trust is implementing and deploying privacy-ABCs in two actual production pilots. These two user-trials will give the opportunity for the first time to test credentials use and performance on a large scale and provide experiences on their operation, interoperability and user acceptance. The first pilot scenario will be deployed at a school in Soederhamn, **Sweden**, where young students (youngsters and teenagers of both sexes) will be able to communicate in an anonymous and privacy preserving way with other pupils and with school health personnel (doctors, nurses, psychologists and other coaches). The second pilot scenario will be deployed at the University of Patras, **Greece**, where students will be able to anonymously evaluate courses they attended.

Thus, ABC4Trust is building its architecture based on privacy requirements collected within the European setting (e.g. Greece and Sweden). However, privacy concerns differ in the international setting. These differences can be attributed to differences in cultural values and perception of privacy, differences in the familiarity with Web privacy practices, or even differences in regulations. In that respect, international cooperation could greatly help exchanging views with other cultures, collect different application scenarios and requirements from other cultures and effectively broadening the perspective of privacy-ABC architecture.

It is, therefore, an open research question to be discussed how privacy relevant processing with and in countries like Brazil, India or South Africa can be handled within ABC-scenarios. How are concepts like proportionality, unlinkability, minimal disclosure etc. being perceived in such countries? How other legal systems outside Europe can be affected by and have effects on Privacy-ABCs?

Technological research can also be greatly benefited from international cooperation when it comes to taking under consideration the human factor in designing technologies. How people perceive technological solutions and how that affects the adoptability of the corresponding technologies? How to best explain to people the potentials and features of the existing solutions? How to best design user-interfaces to encourage usability and adoptability? The answers to these questions will vary for different cultures and by opening up beyond the European borders will give us a great insight in these aspects and eventually help us design better technology.

To address the above challenges, collaboration opportunities should allow EU-project consortia to open up and include various kinds of actors in the international setting: user communities, governmental organizations, regulatory authorities, and research institutes. A framework for enabling such collaboration should encourage joint working groups, organization of public events with experts from both sides and collaboration in standardization activities.

Human-oriented approaches to trust, security and privacy and the role of international cooperation – John Zic

John Zic is a research team leader in the Commonwealth Scientific and Industrial Research Organisation (CSIRO) ICT Centre, specialising in the area of privacy, security and trust. He is a co-inventor of the patented Trust Extension Device, which was the world's first portable USB trusted computing platform to incorporate a TPM cryptographic microcontroller. He holds Honorary Senior Research Fellow positions at the Department of Computing, Macquarie University and with the School of Computer Science and Engineering, UNSW. John has recently given invited presentations and keynotes at the EU FP7 INCO-TRUST workshop in New York in 2010, MIT Kerberos Consortium Conference in 2010 and 2011, and the Vanguard/TTI CyberINsecurity Conference in 2010 and participated in the 11th Joint EU and Australian Science and Technology Cooperation Committee in 2010. John was a member of the Australian Academy of Technological Sciences and Engineering Working Group on Cloud Computing from 2009-2010 advising on privacy, security and trust.

Fundamentally, the basis for human oriented approaches to trust, security and privacy relies on having a real (recognized) need for people to work together on a work package that cannot be addressed by a single entity. By grounding and focusing the work within a collaborative setting, a solid, practical understanding of the requirements for trust, security and privacy may be developed.

Further, partner organisations (commercial, government, and academic) will understand how best to contribute their own respective capabilities within the collaboration. To emphasise that there is a continuum of requirements for trust, security and privacy, two case studies were presented: one dealing with a specialist committee to respond to Australian biosecurity issues, and the other dealing with smart infrastructure and the relationships between residential customers and service providers. These two cases were used to demonstrate the diversity of collaboration types.

It is important to note that underpinning any successful collaboration requires not only that the partners understand their respective roles and contributions, but can also properly commit their respective resources and fund the work.

Establishing international co-operation is important in two respects. First, it offers collaborating partners increased access to potential receptors for ideas and cross-fertilisation of markets. Second, by definition, it builds a larger research community, and this in turn can enable future, potentially larger/more complex collaborative projects in trust, security and privacy. However, alignment and commitment is required at multiple levels, from the individual researchers to their respective organisations and to the participating governments. This complexity should be in the first instance address in a methodical manner.

First, identifying partners who are like minded and interested in addressing similar, relatively small scale but concrete problems with real needs (such as addressing the information management and process requirements of the biosecurity community). These can be regarded as pathfinder projects, which stand a good chance of being identified, proposed and finally supported by the broader community. Of course, any such project requires funding and commitment from each partner, and in the case of international co-operation,

agreements need to be in place between the respective governments to allow the collaboration to proceed. This is particularly significant, as success requires the respective governments' policies and budgets to agree to participate in the international collaboration.

Actions that can be taken to build international co-operation include the development and building of local expertise and a community of users through such path-finder projects. The success of these is then used to promote further development of international collaborations to the broader community. Path-finder projects may also be used to build up international linkages on an incremental level, with the community of users developing internal and external trust in each other to be able to successfully work together. As part of the community building, the development and engagement of partners in formal forums (such as the Internet of Things Forum, for example) is very important, with regular face-to-face meetings (both formal and informal) occurring during these fora. Once again, as a part of the community building exercise, it is important that each potential partner is able to support the work through assuring some funding and resourcing is set aside specifically for this activity. Good will is necessary, but not sufficient, for ensuring a successful collaboration or community building exercise.

Collaboration with Africa / BRICS for human oriented approaches to security, privacy and trust – Jan Eloff

> **Speaker: Jan Eloff** is currently appointed as Research Director at **SAP Meraka UTD / SAP Research Pretoria** and as an Extraordinary Professor in Computer Science at the University of Pretoria. At the University of Pretoria, he is a co-founder of the Information and Computer Security Architectures (ICSA) research laboratory. He represented South Africa as an expert member on IFIP Technical Committee 11 (Information Security).

Although traditional / developed world ICT markets will experience growth in the future, the growth will be relatively slow since these markets are widely saturated. The next big growth market will likely come from areas that are seen as under-developed, such as the Africa / BRICS region, where ICT use is currently at comparatively low levels.

To ensure that the potential of the Africa / BRICS market can be addressed, it is necessary to understand the needs and challenges of this market. International cooperation between European and Africa / BRICS partners is therefore necessary to establish this understanding and to create solutions appropriate for the target market.

To begin this cooperation, we provide the following recommendations with regards to the research and technology outputs as well as with regards to the collaboration methodology.

Recommendations for cooperation - research and technology outputs

Collaboration should be based on context awareness. Traditional user-centered approaches for technology development do not consider cultural and contextual needs. This results in deriving user requirements that do not give the right view of the real needs, leading to technology failure. Example of contextual factors that should be considered include:

- Cultural norms and tradition
- Appropriate tactics for community entry and engagement
- Appropriate research techniques that involve the users and communities
- Appropriate needs assessment practices
- Infrastructure capacity of the targeted community
- Solution maintenance costs

The technology developed should be advantageous from the viewpoint of the local users. Therefore, technology development should be based on an understanding of the real requirements as well as an understanding how existing technology can be adapted to meet contextual requirements. Lastly, solutions developed should be relevant to local users, their needs and the available infrastructure.

Recommendations for cooperation - collaboration methodology

European funding opportunities (e.g. Framework Programmes) should encourage
collaboration with partners in Africa / BRICS. European Project consortia should be more open to accept African / BRICS partners, which should not just provide use cases, but should also develop and adapt technology for their local needs.

We also recommend the following three areas of research topics for international cooperation with regards to security, privacy and trust.

1. Research topics for international cooperation - Security

In Africa / BRICS, mobile phones are the most common ICT device used. Typical users of such devices may not fully understand the security vulnerabilities the use of these devices pose. Security configuration of such devices for most users will therefore be a challenge. Therefore, the research challenge to address with regards to facilitating usable security is: How to quantitatively analyze and design appropriate user interfaces for mobile devices to enable a typical user to make informed decisions about different security settings?

2. Research topics for international cooperation - Privacy

Privacy and information utility are conflicting requirements. As the level of privacy increases, the level of information utility decreases. This is because as we hide more information to preserve privacy, the usefulness of the released information decreases. Local context and culture also influence what information should be regarded as private, and what information is considered as useful. Therefore, the research challenge to address with regards to privacy is: How to ensure an optimum balance between privacy and utility, taking into account local contextual needs and preferences?

3. Research topics for international cooperation - Trust

In African communities, trust is influenced by social network position. Social position governs activities within rural communities. For example, the chief of a village can influence business collaborations. Rural communities therefore require a different approach to business due to unique social structures, social norms, and traditions. Therefore, the research challenge to address with regards to trust is: How to ensure that trust management takes into account concepts relevant to the target context?

Conclusion

In conclusion, by facilitating international cooperation to provide human oriented approaches to security, privacy and trust, we believe that both European and African / BRICS partners will benefit. The great potential of the Africa / BRICS market can be exploited, while at the same time, these markets will be provided with solutions that are appropriate, affordable and contextually-relevant.

Network of Excellence on Engineering Secure Future Internet Software Services and Systems – Fabio Martinelli

Speaker: Fabio Martinelli is a senior researcher in the security group at Security Group at the Istituto di Informatica e Telematica - IIT; National Research Council - C.N.R. He is the Project Coordinator of the EU Project NESSoS Network of Excellence on Engineering Secure Future Internet Software Services and Systems and responsible for the CNR Interdipartimental Security Project.

The Network of Excellence on Engineering Secure Future Internet Software Services and systems (NESSoS, http://www.nessos-project.eu) aims at constituting and integrating a long lasting research community on engineering secure software-based services and systems.

The NESSoS engineering approach of secure software services is based on the principle of addressing security concerns from the very beginning in system analysis and design, thus contributing to reduce the amount of system and service vulnerabilities and enabling the systematic treatment of security needs through the engineering process. In light of the unique security requirements the Future Internet will expose, new results will be achieved by means of an integrated research, as to improve the necessary assurance level and to address risk and cost during the software development cycle in order to prioritize and manage investments. NESSoS will integrate the research labs involved; NESSoS will re-address, integrate, harmonize and foster the research activities in the necessary areas, and will increase and spread the research excellence. NESSoS will also impact training and education activities in Europe to grow a new generation of skilled researchers and practitioners in the area. NESSoS will collaborate with industrial stakeholders to improve the industry best practices and support a rapid growth of software-based service systems in the Future Internet.

NESSoS research topics cover several main areas: A first set of activities represents the traditional early stages of (secure) software-services development: from secure **requirements** over **architecture** and **design** to the **composition** and/or **programming** of working solutions. These three activities interact to ensure the integration between the methods and techniques that are proposed and evaluated. In addition, NESSoS research programme adds two horizontal activities that span the service creation process: Both the security **assurance** programme and the programme on **risk** and **cost** aware SDLC will interact with each of the initial three activities, drive the requirements of these activities and leverage upon, even integrate their outcome; finally, notice that all 5 research activities mentioned above will be inspired and evaluated by their application in specific FI application scenarios.

NESSoS considers necessary a Networking and Liaison Board (NaLAB) for international cooperation mainly aimed at representatives of Technical WGs in the topics of the NoE. The creation of the NaLAB is in progress right now and it is explicitly meant to collect researchers from outside Europe. Several NESSoS components would benefit the international cooperation: The NESSoS Common Body of Knowledge, the engineering tool workbench, open competition, research activities. NESSoS plan to identify the main stakeholders in the NESSoS topics world-wide and create connections among researchers/WGs especially using the NESSoS internal mobility programme. Some possible cooperation topics include comparison of tools and techniques; Usage control of disseminated data; and focus on SLA with protection information, possibly in cooperation with other projects as ASSERT4SOA and ANIKETOS.

NESSoS use cases covers smart-GRIDs and e-heath scenarios. We think that those are currently hot topics and cooperation at international level fruitful.

Panel Session 3. Digital ecosystems network and information security and how international cooperation can provide mutual benefits – Chaired by John C. Mallery on behalf of Karl Levitt

International Data Exchange and A Trustworthy Host: Focal Areas For International Collaboration In Research And Education – John C. Mallery

Speaker: John C. Mallery, Massachusetts Institute of Technology, Computer Science & Artificial Intelligence Laboratory, Cambridge, MA, United States
John C. Mallery is a research scientist at the Massachusetts Institute of Technology, Computer Science & Artificial Intelligence Laboratory. He is concerned with cyber policy and has been developing advanced architectural concepts for cybersecurity and transformational computing for the past decade.

A key message is the acknowledgement that international cooperation is nascent and a more global approach is urgently needed because there is ultimately just one, single global information environment, consisting of the interdependent networks of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.

Table 1 enumerates asymmetries within cyber attack and defense that today disproportionately favor the attacker. The attacker benefits from the initiative (A) and the large defender value at risk (B), whereas the defender controls more knowledge (L), architects the systems (M) and the criminal justice system (N). In between (C – K), the attacker has many advantages but international data sharing and defensive coordination can deny advantage to the attacker by improving communication (F), enhancing situational awareness (G), providing mechanisms for coordination (I), speeding up decision cycles (J), increasing agility (K), encouraging more defensible architectures (M) and supporting or incentivizing defensive coordination with the legal system.

Table 1. International data exchange can reduce asymmetries between attack and defence.

	Mode	*Attacker*	*Defender*
A	Initiative	Chooses the best place, time and means of attack	Must defend everywhere, all the time, against any attack
B	Value At Risk	Small (terror or criminal actors)	Large
C	Code Size	Small (often 100s of lines)	Large (>20-50 million lines)
D	Software Control	High	Supply chain → Low
E	Software Abstraction	Good, integrated for purpose	Poor, evolutionary tower
F	Communication	Organized around attack → Good	Organized around products → Poor
G	Situational Awareness	High	After-market bolt-on → Low
H	Accountability	Low (terror or criminal actors)	High
I	Coordination	Small group → high	Non-scalable → low
J	Decision cycle	Fast	Slow
K	Agility	High (apparent)	Low
L	Domain Knowledge	Low, narrow & concentrated	High, broad but diffuse
M	Architectural Control	Low	High, but slow
N	Legal/Justice Systems	Low	High, but slow & political

It is essential that we have the ability to conduct comprehensive intelligence collection and evaluation on any developing situation that threatens our cyberspace activity, followed by near-simultaneous processing, exploiting and disseminating of the information. This depends on collaboration, data exchange and sharing (and also knowledge sharing) between countries. We need comprehensive research towards international intelligence, surveillance, and reconnaissance (ISR) in the cyberspace domain.

Mallery characterized these challenges as follows.

- **Problem:** Attackers can replay attacks across different countries without rapid international learning to defend against attacker innovations
- **Benefits:** International collaboration and coordination can rapidly reduce defensive gaps across the OECD and build crisis-response capacities
- **Leverage:** Bias work factors in favour of defense and against cyber attack
- **Approach:** Exchange data related to cyber crime, attack patterns and best defense practices
- **Research:** Motivate technical research via needs of realistic data sharing scenarios

An architecture for international and cross-sector sharing of cyber threat and attack data will ensure a more effective collective cyber defense than countries, sectors or organizations might otherwise achieve individually.

Fig. 1. Straw man architecture for international data sharing and collaboration.

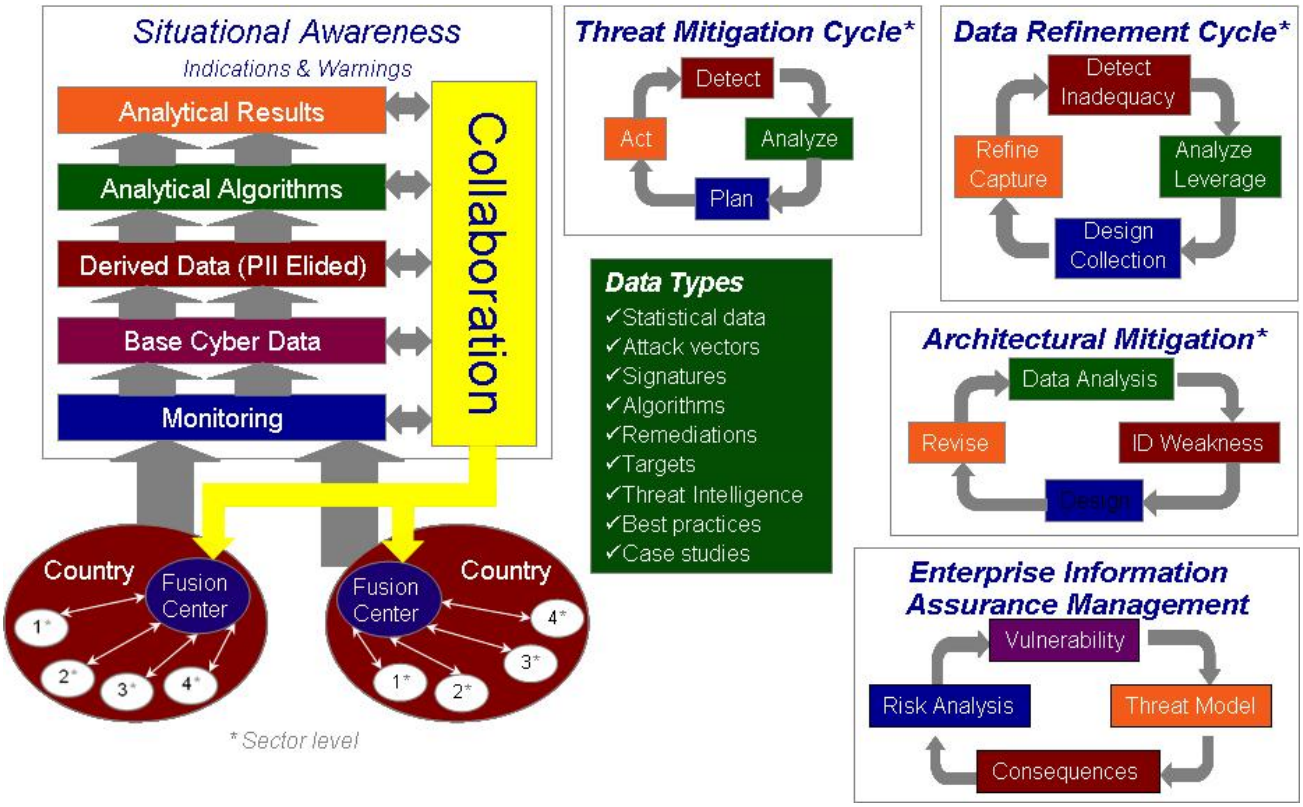

Figure 1 illustrates an international cyber data sharing architecture that integrates data from multiple countries and sectors and returns collaboratively produce analytical products and threat mitigation techniques. Country fusion centers integrate country information and expertise internationally. Within each country and across its sectors, shared monitoring infrastructures capture base cyber data at sources. This data is processed to remove personally identifiable information (PII) before being analyzed using shared algorithms to produce results fed back into shared situational awareness. The architecture supports sector-based threat mitigation cycles as well as enterprise information assurance management of value at risk. The architecture supports learning modalities like data refinement to improve data capture, analysis and utility in threat mitigation. Based on knowledge gained about vulnerabilities and attacker vectors, the architecture helps drive improvement of enterprise and infrastructure architectures to improve defensibility.

This kind of sharing scenario can drive research along many trajectories. The type of data collected needs to be effective and offer leverage for cyber defense. Large-scale analytics over the data need to reveal important patterns in real time and lead to timely threat mitigation. Given an effective sharing architecture, major malicious actors will endeavor to corrupt the data and subvert its operation, and so resilient and trustworthy engineering will be needed for all components from sensors to hosts, monitoring, analysis and mitigation actions. At the same time, PII and enterprise information must be protected to respect important societal values and incentivizing sharing. Difficult technical, legal and administrative challenges in international authentication, authorization, encryption and remote policy enforcement must be overcome to reach higher levels of trust and sharing necessary for weaponizable data like critical infrastructure attacks and mitigations.

Mallery characterized the goals of cyber data sharing and collaborative analysis as follows:

- Build shared awareness and understanding of cyber phenomena across countries
    - Employ shared data collection methodologies
    - Integrate measurements of phenomena across borders
    - Focus early on cyber crime and economic incentives
- Create comparable transnational data sets
    - Capture cyber breaches, attack patterns, best practices, defensive coordination
    - Include aggregate data on crime, black markets, economics, state-state interactions, long-term transformations
- Field a cyber data sharing framework that helps countries to:
    - Collect cyber data for compatible sharing
    - Fuse data to create common situational awareness
    - Manage national legal impediments to sharing via derived or aggregate data or by recommending harmonization steps
    - Exchange derived data in real time

    - Provide mechanisms for controlled drill down needed for law enforcement, advanced persistent threats (APT) or cyber emergencies
- Build shared collection, fusion, analysis, and response capabilities

In addition to cyber data sharing and collaborative analysis, Mallery introduced the idea of raising the work factors for malicious actors worldwide by collaboratively developing an open-source trustworthy host platform for collaborative research and education. Mallery characterized the challenge as follows:

- Problem: Attackers are subverting legacy architectures which are inadequate for current threats
- Benefits: Development and evolution of a clean-slate trustworthy host will:
    - Create reference host architecture for computing, routers, cloud, embedded, wireless
    - Integrate best information assurance (IA) engineering from the open literature
    - Provide a reference paradigm for cumulative research and education
    - Drive higher assurance for open source and commercial software
- Leverage: Raise work factors required to compromise commodity hosts
    - Eliminate remote access penetration vectors
    - Prevent privilege escalation
    - Manage information leakage
    - Verify tool chain and resulting software
    - Rapidly detect and remediate flaws or breaches
- Approach: Pool research efforts across OECD countries to create and evolve a shared host platform reflecting best IA engineering practices
- Research: Motivate technical research via needs of an existing and readily-accessible free implementation

Finally, Mallery presented 10 technical features for a trustworthy operating system.

1. Safe Language*: No penetration vectors
    - Clean semantics – lambda calculus, extensible
    - Design for verification
    - Composability (practical even if incomplete)
2. Trusted Operating System*: Enforce least privilege
    - Separation kernels or hypervisors
    - Factored into well-defined independent cooperating components
    - Critical components verified
3. Binary Hygiene*: Eliminate return oriented programming
    - Control function entry/exit points (gates)
4. Information Flow Control: Manage side channels
    - Leak resistance
5. Monitoring: Audit & Accountability
    - Multi-scale reference models

- Privacy awareness

6. Recovery: Efficient diagnosis and rollback to known states
   - Transactional persistent memory
7. Safe Networking Stack: Enforce least privilege
   - Protocol and channel separation by application, process or thread
8. Authorization & Authentication System: Manage least privilege
   - Non-by-passable
9. Separation User Interface:
   - Manage domain crossings explicitly
10. High Productivity Trusted Software Engineering*:
    - Inside industry development Cycles
    - Verified tool chain

During the discussions, Bart Preneel suggested cryptographic software stack as an additional requirement and everyone agreed.

International Cooperation on Cryptology – Bart Preneel

Speaker: Bart Preneel is a full professor in the research group ***COSIC*** of the ***Electrical Engineering Department*** of the ***Katholieke Universiteit Leuven*** in ***Belgium.*** His main research area is information security focussing on cryptographic algorithms and protocols as well as their applications to computer and network security and mobile communications.

Professor Bart Preneel presented the **ECRYPT II** project[25], a Network of Excellence project in Cryptology with 11 partners and 25 associate partners (1 from Taiwan). *ECRYPT II,* which stands for *European Network of Excellence for Cryptology II,* is a 4-year network of excellence funded within the Information & Communication Technologies (ICT) Programme of the European Commission's Seventh Framework Programme (FP7) under contract number ICT-2007-216676. It falls under the action line *Secure, dependable and trusted infrastructures*. ECRYPT II started on 1 August 2008 and runs until the end of 2012. Its objective is to continue intensifying the collaboration of European researchers in information security.

The main objective of ECRYPT II is to ensure a durable integration of European research in both academia and industry and to maintain and strengthen the European excellence in these areas. In order to reach this goal, 11 leading players and 20 adjoint members to the network propose to integrate their research capabilities within three virtual labs focusing on symmetric key algorithms (SymLab), public key algorithms and protocols (MAYA), and hardware and software implementations (VAMPIRE). ECRYPT II has been publishing widely used yearly report on algorithms and key lengths.

Some of the technical objectives of ECRYPT II include improving trade-offs between cost (footprint, power and/or energy consumption), security and performance**;** development and analysis of advanced cryptographic protocols for distributing trust**;** and secure hardware and software implementations**.**

The ECRYPT II research roadmap for the next 10 years is motivated by the changing environment and threat models in which cryptology is deployed and has a focus on Crypto for Internet of Things including the need for low energy crypto; Crypto for cloud computing including distributed cryptography; fully homomorphic encryption; cryptology for use in applications (in part driven by regulation) e.g. privacy for smart grid; privacy for road pricing; e-voting; and advertising.

In terms of the key elements required for the cryptology area on an international level, there is a need for an integrated policy at EU level and international collaboration is required across academia, industry and government agencies and there is a significant need for collaborative research and its interaction with policy. To build an international strategy for INCO, there is a need for collaboration on cryptographic algorithms with the forging of open competitions with shared governance; effective standardization and continual

[25] **http://www.ecrypt.eu.org/**

updates of a key lengths and parameters document (management of standards). Collaboration also should take place on cryptographic protocols motivated by distribution of trust and privacy (key component in privacy by design) and joint research also need to occur in these areas. We can be more effective by avoiding duplication and increasing impact on both the technology and policy levels. Professor Preneel concluded by saying it was good to see that Cryptology is included in the research agenda presented earlier within the identified BIC topics.

Trust & Security for Mobile Communication Services – EU- India cooperation – Abhishek Sharma

Speaker: **Abhishek Sharma** is Co-founder, MD & CEO of NetEdge Tele-Solutions (NTS). He is a veteran of the ICT domain with authority on Telecom & Radar. Abhishek has a B.E. Degree in Electronics & Telecom Engineering, from GEC, Jabalpur, M.E. in Computer Sc & Automation from I.I.Sc, Bangalore, Masters in Management Studies from College of Defense Mgmt & M.B.A. in Marketing from IGNOU Delhi. His company develops mobile applications on Utility VAS for GSM/ CDMA mobile users. Abhishek is also international consultant on Mobile VAS, Telecom Network, Radar Data Systems and Avionics. He has rich experience of managing large business, Operations & projects, setting up GSM, CDMA, Satellite & Radar NW and BSS, OSS solutions. Abhishek has participated in many national 7 international seminars and events and has pitched novel product & solution ideas.

INTRODUCTION

In the world of computers and communications, the more widely a technology is used, the more likely it is to become the target of hackers. Such is the case with mobile technology, particularly Smart Phones, which have exploded in popularity in recent years. Smart Phones becoming very popular among people and a considerable part of the population owns at least one of them. The main reason behind this growing popularity is the availability of variety of applications for them, be it for entertainment, utility or just better user experience. This popularity has attracted enough hackers to make the potential for serious security threats a reality. McAfee Labs' threat report for 2010's fourth quarter reported a 46 percent increase in malware targeting mobile phones over the same time period the previous year. More than 55,000 new pieces of malware are seen on a daily basis as per the report. Visiongain research shows that the number of mobile malware more than doubled in 2011 from 2010 with over 200 new variants in the first half of 2011 alone

Mobile devices are the fastest growing consumer technology, with about 600 million smart phones today to crossing 1.74 billion by the year 2012. Mobile applications are likewise booming. In June 2011, for the first time ever people on average spent more time using mobile applications (81 minutes) than browsing the mobile web (74 minutes). With this scenario, Mobile devices increasingly face various types of threats from mere Annoyance to invade privacy, propagation, malicious tools or Steal Money. Threat to mobile money transactions could be one of the most dangerous and painful security threat. The value of mobile payment transactions is projected to reach almost $630 billion by 2014, up from $170 billion in 2010[5]. Vendors, retailers, merchants, content providers, mobile operators, and banks are all actively establishing new payment services. Mobile payments create an attractive target for attackers, as they allow direct monetization of attacks.

MOBILE SECURITY THREATS & MOBILE APP VULNERABILITY:

Security Threats: It important to analyze the sources of such threats besides analyzing the vulnerability. Mentioning a few major ones – **Botnet**, which is a collection of compromised devices connected to the Internet. The malware gives hackers remote control of the compromised devices, which can then be instructed to perform harmful acts. The easiest way for an attacker to benefit

from a mobile botnet is to send SMS or multimedia message service (MMS) communications to a premium phone account that charges victims fees per message. **Malicious applications** are usually free and get on a phone because users voluntarily install them. Once on a handset, the programs steal personal information such as account passwords and logins and send it back to the hacker. **Social Networking** has grown enormous as smart phone use has grown, so has mobile Malicious links on social networks can effectively spread malware. Participants tend to trust such networks and are thus willing to click on links that are on "friends'" social networking sites, even though a hacker may have placed them there. **Spyware** available online are used to hijack a phone by hackers, allowing them to hear calls, see text messages and e-mails, and even track a user's location through GPS updates. Bluetooth enables direct communication between mobile devices. Wireless devices can broadcast their presence and allow unsolicited connections. Though on rare occasions, mobile malware has used Bluetooth to propagate. In case of Wi-Fi Hackers can intercept communications between smart phones and Wi-Fi hotspots. In this scenario with has no encryption to protect transmitted data., the hacker gets between the user and the hotspot provider and hijacks the session via a man-in-the-middle attack. **Phishing** poses the same risk on smartphones as it does on desktop platforms. Mobile phishing is particularly tempting because wireless communications enable phishing not only via e-mail, as is the case with PCs, but also via SMS and MMS. Social media phishing is becoming a major issue as social networking sites contain an increasing amount of personal information.

App Vulnerability: Like traditional applications for desktop / laptop computers, mobile apps too suffer from myriad security vulnerabilities. Many of these vulnerabilities are unintentional, caused by poor programming practices. Vulnerabilities can also be intentional and malicious, hidden within a seemingly safe and legitimate app. Some security vulnerabilities occur when sensitive data is transmitted to and from remote servers over unencrypted channels. Perhaps the most severe app vulnerabilities are those that exploit lax security of stored data.

SECURITY APPROACHES

Traditional Security Approaches: Mobile communications can use the same types of security-antivirus and firewall products as fixed communications. Vendors include Fortinet, F-Secure, Juniper Networks, Trend Micro etc. Mobile security software can also better use the cloud to offload some of the processing.
Mobile Encryption software is another approach but there are only a few such as Cryptech by Caspertech, Cellcrypt by Cellcrypt Mobile, ComSecure by NetEdgeTeleSolutions, Phonecrypt. They're scarce primarily because they're challenging and expensive to develop.
Vetting the Apps by Purchasing organizations or a third-party labs before buying them is another approach. . However, the vetting process poses several challenges, including specifying security and analysis requirements; identifying appropriate tools, mechanism, and approaches for analyzing security vulnerabilities and finding appropriate personnel to manually vet the apps. To foster the availability of only "safe" apps, it's also necessary to vet the app store.

However Before you can analyze an application, you need an infrastructure for testing the application and reporting the results.

STATUS & DEMAND

Currently, app stores don't incorporate a vetting process that thoroughly examines potential security vulnerabilities in apps made available to consumers. This is likely due in part to the cost and time associated with vetting an app, as well as the potentially complex and contentious interactions needed with developers to resolve identified vulnerabilities. Given the growing potential for dangerous and widespread vulnerabilities, however, it's becoming increasingly critical to vet apps for such vulnerabilities, but in a cost- and time-efficient manner.

As the mobile ecosystem evolves and hackers probe for vulnerabilities, devices will face a growing number of a variety of attacks viz a viz those traditionally launched against desktop systems. The need is to increase analyzing the attacks. The greater visibility of these attacks will place an increasing importance on mobile device makers to include security features and configuration options in place. Also to make it necessary that security is to be considered in all phases of application development to ensure that resiliency against attacks is built into mobile devices from the start.

Commercially, the global market for Mobile Security is projected to reach $14.4 billion by 2017, primarily driven by rapid proliferation of feature phones and intelligent mobile computing devices. Increasing use of mobile devices for accessing data services and corporate networks and the emergence of open network concept, which opens up potential risk avenues from security and privacy perspective will boost market prospects over the next few years. Robust demand from Asia-Pacific market also augurs well for the future of this market.

CONCLUSIONS

In future, there will be significantly more confidential operations like banking transaction, mail exchanging will take place from mobile only. In these cases, it is very necessary to protect the customer data and application from various attacks. Since the Smartphone/ Mobile penetration is increasing globally, it makes a lot of sense that large regions, particularly regions like Europe and India/ Asia collaborate closely for the Research & Industrial Developments. Many companies are already putting efforts in making their consternation for securing mobile data and application.

Finally, it's critical to understand what there is to lose before a mobile security breach occurs. The ultimate goal is not about completely eliminating mobile security risks but rather having the proper systems in place to minimize the impact when breaches occur. Well thought out controls involving the proper security technologies combined with the proper documentation and business processes are essential.

BIC CONTRIBUTION

Today, the realisation has come and lots of efforts are in progress at different locations, organisations & institutions and different levels towards addressing the issues related to Trust & Security. There is also lots of focus towards mobile

Security. However all these efforts are happening largely in isolation and wherever there is any cooperation and coordination between different organisations, it is very limited. Focussed and targeted international cooperation shall play a major role in this massive & coordinating efforts for research, development and implementation of measures required to be taken to address this menace of the “breach of Trust & Security for Mobile”. Towards this, BIC can and have to be a key player in ensuring this critical coordination. Following actions are suggested:

- Increase the degree and level of Industry participation from the level where it is today.
- An appropriate combination of SMEs and large corporate with balanced mix with research bodies would be ideal.
- Suitable selection criteria, based on result orientation & capabilities of the participants may be worked out.
- Special incentive coupled with delivery commitments be accorded to SMEs who are more oriented and geared up for faster deliveries.
- Increasing the frequency of interactions by way of seminars and events.
- Create a Project Management Team or a sub group under the Programme Manager, comprising of representatives from Institutions and industry (SME & Corporate) with defined leadership, targets & timelines.

A mobile has already become a full time companion. Soon it shall be a full time friend, philosopher & guide and all in one service provider. Most of the “Delivery of Services” shall happen through mobile, world over. It would not be any exaggeration to say that these are “desperate” times ensuring “Trust & Security for Mobile” and *desperate times need desperate measures.*

EU-US joint CIIP Exercise, Cyber Atlantic 2011 – Raznan Gavrila

> **Speaker: Raznan Gavrila** is the Network and Information Security Operation Officer, CIIP & Resilience Unit, at European Network and Information Security Agency (ENISA).

The European Union's cyber security agency, ENISA[26], organised an EU – US Joint CIIP exercise, called Cyber Atlantic 2011, which was held on 3rd November 2011. The idea for this exercise was discussed during a number of events and initiatives including: EU-US summit of 20 November 2010 (Lisbon); EU-US Working Group on Cybersecurity and Cyber Crime (EU-US WG). The holding of the event was formally announced on 15th April 2011 during the Hungary Ministerial Conference by Commissioner and DHS Secretary and ultimately held on 3rd November 2011.

Cyber Atlantic 2011 was the first joint EU-US cyber exercise and was comprised as a centralised table-top exercise in which over 20 countries were involved (17 countries played). The overall planning and preparation was carried out by ENISA and DHS incorporating facilitation and overall management of the preparation and evaluation phases. The planners teams were from: AT, BE, EE, ES, FI, FR, HU, IT, NL, RO, SE, UK, ENISA, US/DHS, EC, JRC.

Cyber Atlantic 2011 was an exercise of an exploratory nature with the following objectives:

- Explore and identify issues in order to improve the way in which EU Member states would engage the US during cyber crisis management activities;
- Explore and identify issues in order to improve the way in which the US would engage the EU Member states during their cyber crisis management activities, using the appropriate US procedures;
- Exchange good practices on the respective approaches to international cooperation in the event of cyber crises, as a first step towards effective collaboration.

There was a two part scenario: Advanced Persistent Threat (APT) scenario with a hacker group, "Infamous" exfiltrated sensitive documents from EU and US – 'Euroleaks' web site and Supervisory Control and Data Acquisition (SCADA) scenario highlighting vulnerabilities leading to backdoors (and failures) on Programmable Logic Controllers of power generation equipment.

The lessons learned (tentative) from Cyber Atlantic 2011 were:

- Mechanisms/structures for cross-border cooperation do exist; however, each country needs awareness of all communications options ;
- Exchange Standard Operation Procedures (SOPs), trainings, exercises;
- Exercises need increased participation from all three: Technical, Law Enforcement, Policy/Political;
- Single Point of Contact in EU for US would help but is not compulsory;
- More exercises/workshops are needed!

[26] http://www.enisa.europa.eu/

Information Security by NICT and the Government of Japan - Hiroyuki HISHINUMA

Speaker: Mr. Hiroyuki HISHINUMA is currently Director of Europe Center, **National Institute of Information and Communications Technology (NICT),** which is a research institute of ICT in Japan. Before he came to NICT, Mr. Hishinuma worked in the Ministry of Internal Affairs and Communications (MIC), the Government of Japan, dealing with telecommunications policy.

1. Information Security Policy by the Government of Japan (MIC: Ministry of Internal Affairs and Communications)

MIC has developed an information security policy consisting of four aspects; network, individuals, technology and international partnership & collaboration.

As a solution to fight against cyber attacks, MIC started a new project based on international collaboration in this April. The project aims at gathering research institutes, ISPs and other experts, and the project establishes an information-analysis and -sharing system that utilizes cyber-threat data, gathered through various sources.

MIC wants to implement various effective activities with collaborating partners, including information exchange, joint R&D, etc., on various levels, such as the government, research institute and operational level. MIC hopes other countries to be a collaborating partner.

2. R&D on Cybersecurity by NICT (NICT: National Institute of Information and Communications Technology)

NICT researches and develops “nicter”, that is Network Incident analysis Center for Tactical Emergency Response. “nicter” is the largest network monitoring system in Japan. In the nicter, Macro analysis System is a darknet monitoring and analysis system. Micro analysis System is a fully automated and isolated malware analysis. Network and malware enchaining system binds phenomena (or attacks) and root cause (or malwares). Then candidates of infecting malware can be listed.

Among the Macro analysis System in ”nicter”, Mr. Hishinuma demonstrates geographical traffic visualization, which shows geographical positions of a packet’s source and destination from the IP addresses in real time.

NICT is conducting Research and Development to investigate practical Cybersecurity technologies. NICT still needs new frameworks to monitor, analyze and respond the emerging threats. International collaboration is crucial for Cybersecurity field.

3. Discussion

Mr. Hishinuma was asked whether MIC has already started cooperation with other countries on the new project. Mr. Hishinuma answered that discussions for collaboration with EU, France, U.K., and ASEAN countries are going on. His colleague in NICT has just visited South Korea to collaborate with this in the last week.

Annex III. Report of the BIC Annual forum planning session held on 6TH July 2011

Building International Cooperation for

BUILDING International Cooperation for Trustworthy ICT

European Commission
Information Society and Media

BIC Partners

TSSG

Waterford Institute of Technology

TECHNISCHE UNIVERSITÄT DARMSTADT

TELECOM ParisTech

Atos

BIC planning session on

Building a long term International Cooperation strategy in Trustworthy ICT

System Security and Cyber-Defence: requirements for an international approach to technological challenges and open issues.

Amsterdam, Netherlands

6th July 2011

Table of Contents

EXECUTIVE SUMMARY

The EU FP7 BIC project [1], with the support of the SysSec project [2], organised a session as a step in the development of plans and proposals for international collaboration in research towards a vision of cyber-space that supports fundamental freedoms, privacy and the free flow of information in a secure and reliable manner, while protecting the essential information infrastructures on which we depend.

The session was held on 6th July 2011, during the afternoon of the SysSec workshop. The stated objectives of the session were:

- Address the general question of the scope and priorities, and initial planning considerations for international collaboration on R&D towards trustworthy ICT.
- Explore *Frameworks for Data Sharing*, as a specific enabler for collective defence and response to cyber-attack.
- Prepare the ground for the extended BIC workshop being planned for, Quarter 4 2011;
- Further clarify scope for international collaboration on cyber-security;
- Progress the Secure International Data Exchange Architecture for Cybersecurity, introduced at the May, 2010 workshop to explore the technical and organisational requirements and constraints.

Due to the nature of the SysSec workshop and expertise of the participants, the BIC session organisers placed a heavy emphasis on the continuation of the work started during the Inco-Trust project on scoping an International Data Exchange architecture, specifically for cybersecurity, which would enable exchange and sharing between responsible states and organisations of information and intelligence on cyber-attacks. The participants feel this would be an essential component of collective cyber-defence against malicious action (as well as accidents and flaws). It is central to the ability to anticipate and respond: longer-term in the preparation of strategic, collective defensive measures, and short-term in recognising, isolating, and recovering from, attack – threatened or actual.

The comprehensive ninety minute session was broken into the following sections with expert speakers from around the globe.

1. Motivation and vision
2. Threat models, actors and capabilities
3. Technologies to support the International Data Exchange Architecture
4. Legal, regulatory, political, social, economic, and environmental challenges
5. Next steps for planning

The organising committee of the BIC session included:

Jim Clarke,	Waterford Institute of Technology, IRL
Karl Levitt,	The University of California, Davis, USA
Evangelos Markatos,	FORTH, Greece,
Neeraj Suri,	TUD, Germany
John C. Mallery,	MIT, USA
Michel Riguidel,	Telecom Paris-Tech, France
Aljosa Pasic,	ATOS Origin, Spain
Rebecca Wright,	Rutgers University, USA.

INTRODUCTION, MOTIVATION AND VISION

The quantity and seriousness of cyber attacks have been clearly growing over the past six years and have surged over the last three months. Although there have been real improvements in enterprise cyber defences, threats have been outpacing them. Recent attacks have ranged from spear phishing email accounts to gain footholds into organizations, infiltration of international economic institutions (possibly with insider advantage), and other neo-mercantilist industrial espionage. Added to these are growing ideological hacktivism and a potential threat of cyber terrorism against critical services and infrastructures as terrorist continue to use the Internet to recruit and coordinate.

Cybersecurity is now receiving high priority for international collaboration. Some recent examples are highlighted here:

- EU–US INCO-Trust workshop of May 2010 [3],
- Munich Security Conference, 4-6th February, 2011 [4]
- US-UK Cyber Communiqué of 25th May 2011[5],
- Recent accession to the Budapest Convention on Cybercrime [6],
- 28th Annual International Workshop on Global Security on June 16, 2011 [7], and
- Vienna Security conference, 1st July 2011 [8].

A key message throughout all of these events is the acknowledgement that international cooperation is nascent and a more global approach is urgently needed because there is ultimately just one, single global information environment, consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.

It is essential that we have the ability to conduct comprehensive intelligence collection and evaluation on any developing situation that threatens our cyberspace activity, followed by near-simultaneous processing, exploiting and disseminating of the information. This depends on collaboration, data exchange and sharing (and also knowledge sharing) between countries. We need comprehensive research towards international intelligence, surveillance, and reconnaissance (ISR) in the cyberspace domain. The anticipated benefits of an international data exchange system include:

- **Data exchange and sharing capabilities** for monitoring of trends with availability of retrodictive cyber statistics across the OECD; enhanced anti-crime counter-measures better identifying cyber crime targets, vectors, methods, and counter-measures; closing defensive gaps with better defensive coordination and best practices; and enhancement of IP protection with the detection and prevention of industrial espionage.
- **Expertise integration** to focus collective expertise on important cyber data and analysis tasks.

- **Collaboration and coordination** reducing defensive gaps across the OECD and better crisis response.
- **Research and development coordination** to leverage and combine national expertise.

Table 1 enumerates asymmetries within cyber attack and defense that today disproportionately favor the attacker. The attacker benefits from the initiative (A) and the large defender value at risk (B), whereas the defender controls more knowledge (L), architects the systems (M) and the criminal justice system (N). In between (C – K), the attacker has many advantages but international data sharing and defensive coordination can deny advantage to the attacker by improving communication (F), enhancing situational awareness (G), providing mechanisms for coordination (I), speeding up decision cycles (J), increasing agility (K), encouraging more defensible architectures (M) and supporting or incentivizing defensive coordination with the legal system.

	Mode	*Attacker*	*Defender*
A	Initiative	Chooses the best place, time and means of attack	Must defend everywhere, all the time, against any attack
B	Value At Risk	Small (terror or criminal actors)	Large
C	Code Size	Small (often 100s of lines)	Large (>20-50 million lines)
D	Software Control	High	Supply chain → Low
E	Software Abstraction	Good, integrated for purpose	Poor, evolutionary tower
F	Communication	Organized around attack → Good	Organized around products → Poor
G	Situational Awareness	High	After-market bolt-on → Low
H	Accountability	Low (terror or criminal actors)	High
I	Coordination	Small group → high	Non-scalable → low
J	Decision cycle	Fast	Slow
K	Agility	High (apparent)	Low
L	Domain Knowledge	Low, narrow & concentrated	High, broad but diffuse
M	Architectural Control	Low	High, but slow
N	Legal/Justice Systems	Low	High, but slow & political

Table 2. International data exchange can reduce asymmetries between attack and defence.

The session speakers were selected based upon their expertise and previous experience in elaborating a comprehensive set of topics related to International cooperation in trust and security. The organizers felt it was very important to also continue the development of cooperation topics from previous interactions so it was decided to use the development of an International Data Exchange Architecture as a clear example of how international cooperation could benefit the trust and security research communities.

On this basis, the final speakers were chosen to introduce the following topics and they were asked to answer the following questions in their talks.

Topic 1. Motivation and Vision: What are we doing and why? What are the expected impacts? What kind of data should we share? What kind of collaborations do we need? What kind of analysis do we need? What are the incentives to participate? What are the risks?

Topic 2. Threat Actors: Who are the threat actors and what are their capabilities? What threat models follow from the actors' business models and capabilities? How are consequences of breach or disruption assessed and their criticality determined?

Topic 3. Technologies to support International Data exchange architecture: Review of the straw man architecture in more detail? What are the enablers eg. Cryptography based obfuscation, sensors on the network, monitoring traffic capabilities? Basics of how we share recognizable data, especially on critical infrastructures and across different countries. eg. share patterns for recognizing advanced persistent threats without losing efficacy if they are exposed? What obfuscation and security measures would make patterns easier to share? Architecting for leakage and resilience under compromise.

Topic 4. Legal, Regulatory, political environment challenges: What challenges arise when dealing across multiple sectors and countries? How are these best addressed at a transnational level? How are legal and regulatory issues including privacy, corporate responsibility best managed in order to improve coordinated defence?

Topic 5. Next steps for planning: What are the concrete next steps until the next event (expected Q4 2011)? How can we motivate countries to contribute and support the effort? More details appear in the agenda (next section).

AGENDA AND SPEAKERS SUMMARIES

Time	Description	Speakers
13:30 – 13:35	Overview / Purpose of Session	Jim Clarke, Waterford Institute of Technology -TSSG
13:35 – 13:55	Part 1. Motivation and Vision: Opening remarks US perspective EU perspective	 Samuel Weber, National Science Foundation, USA Karl Levitt, Univ. of California Davis Barbara Daskala, ENISA
13:55 – 14:05	Part 2. Threats and Actors	Sotiris Ioannidis, FORTH
14:05 – 14:50	Part 3. **Straw man architecture for International data exchange and collaborative analysis** Data exchange architecture used in a financial application in South Africa. Identity related issues for data handling and aggregation	John C. Mallery, Massachusetts Institute of Technology; Barend Taute, The Council for Scientific and Industrial Research (CSIR), South Africa; Glenn Gran, IKED. GINI SA project
14:50 – 15:05	Part 4. Legal, Regulatory, Privacy, and Political Challenges	Jody Westby, Global Cyber Risk LLC, Carnegie Mellon CYLAB
15:05 – 15:30	Part 5. Next steps for planning of workshop in Q4 2011 • Determining a comprehensive coverage of topics required; any gaps? • Identifying key topics for a workshop to be held in the Fall ’11 (see next pages for initial draft terms of reference); • Identify Organising and Program committee; • Identifying the necessary participants; • Identify how to best collaborate between now and then (eg. establishment of working groups, electronic, ….)	BIC partners, interactive

Building a long term strategy for International cooperation in Trustworthy ICT [9]

Speaker: James Clarke, Waterford Institute of Technology, TSSG, Ireland

Since January 2011, James Clarke is Project Coordinator of a European Framework Program 7 Co-ordination action entitled BIC, which stands for Building International Cooperation for Trustworthy ICT: Security, Privacy and Trust in Global Networks & Services. BIC will engage the European Union trust and program management (funding organizations) and research communities with their peers in Brazil, India and South Africa and enable the collaboration with research communities in trust and security already established in the US, Australia, Japan, Korea and Canada established in the recently concluded INCO-Trust project that Mr. Clarke also coordinated from 2008 - 2010. In addition, Mr. Clarke is actively involved in the research community, having served in various international conference committees as organizing, technical and program committee member.

Mr. Clarke opened the session by describing the overall purpose of the BIC session, which was to generate discussions with the systems and network security attendees at the SysSec workshop [10] on addressing the general question of the scope and priorities, and initial planning considerations for international collaboration on R&D towards trustworthy ICT and continue the work started at the May 2010 INCO-Trust workshop [11] on exploring *Frameworks for Data Sharing*, as a specific enabler for collective defence and response to proliferating cyber-attacks.

Mr. Clarke further elaborated the main goals of the session, which are to prepare the ground for the extended BIC workshop being planned for 2011, Q4, discuss with the main stakeholders in attendance to clarify scope for international collaboration on cybersecurity, and continue the good work already started by some of the researchers and to invite others to contribute on the development of a secure International Data Exchange Architecture for Cybersecurity and to further explore the technical and organisational requirements and constraints.

Mr. Clarke described the agenda, which was broken down under a variety of connecting topics, including motivation and vision, threats and actors, technical issues related to the international data exchange architecture for cybersecurity including a strawman architecture, a real life example of a data sharing case for the finance sector and enabling technologies required including privacy protecting identity management, legal, regulatory, privacy and political challenges involved with data exchange and sharing and next steps and planning.

Mr. Clarke concluded by thanking the SysSec workshop organisers for providing the venue for the session and to all of the BIC session organising committee members for the hard work in pulling together the contents of the session. These included John C. Mallery, MIT, USA; Aljosa Pasic, ATOS, Spain; Karl Levitt, The University of California, Davis, USA; Evangelos Markatos, FORTH, Greece; Neeraj Suri, TUD, Germany; Michel Riguidel, Telecom Paris-Tech, France; and Rebecca Wright, Rutgers University, USA.

Opening remarks: International cooperation in Trustworthy ICT [12]

Speaker: Samuel Weber, National Science Foundation, USA

Samuel Weber is in the Directorate for Computer and Information Science and Engineering (CISE) of the National Science Foundation (NSF). Specifically, he is a Program Director in the CISE cross cutting program in Trustworthy Computing.

Dr. Weber presented the National Science Foundation's strategy for international cooperation. Dr. Weber stressed that in addition to NSF, there are other agencies where researchers can look for funding. He emphasised that NSF is not the only funding agency out there. There are many involved in research funding with different missions and priorities and these were highlighted during the presentation. All have different missions but they all coordinated together on a joint strategy in the US research landscape on trustworthy computing. The coordination is carried out by the NCO/NITRD = National Coordination Office for Networking and Information Technology Research and Development (see also the document "Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program").

Dr. Weber described the four main thrusts to the NCO-NITRD* Game-Change Strategy: 1. Inducing Change: within 3 themes

i. Tailored Trustworthy Spaces;
ii. Moving targets; and
iii. Cyber Economic Incentives.

2. Developing scientific foundations.
3. Maximizing research impact.
4. Accelerating transition to practice.

The NSF focuses on long term research and is able and willing to partner with other agencies, who may be looking at more short term research. The NSF is more a bottom up agency where there are broad solicitations from a wide range of topics. For example, these could range from cryptography, operating systems, economics of cybersecurity, and human computer interaction in one big solicitation. The NSF FY 11 funding level is $55M dollars. The ethos of the NSF is to see what people want to research and decide which areas of research need help. They try to spread things out fairly and evolve funding decisions that way.

International cooperation is seen as very important in the NSF, especially from the trustworthy computing perspective. Clearly, different countries have different focuses in which centers of expertise are isolated geographically, hindering everyone. For example, there was a recent RFID security workshop in the US that had many EU people there while other EU based workshops have many US people there. The NSF want to improve the balance by giving more opportunities to those not located in the correct geographical location for their research. For International collaboration, there are different opportunities: *Individual supplements*, support for collaboration: travel, visitors, workshops; *Ad-hoc supplements* in which international proposals can get co-reviews with NSF-equivalents thus avoiding "double-jeopardy" when involving a one review process; and lastly, the harder to obtain *Coordinated solicitations*, which are more focused on solicitation involving multiple agencies on single topics. This is quite difficult to obtain as every agency has different procedures, mechanisms, timing restrictions, but it is possible.

Towards Collaborative Data Sharing – "US perspective" [13]

Speaker: Karl Levitt, University of California Davis, USA

Karl Levitt is a Professor at the University of California Davis. He conducts research in the areas of computer security, automated verification and software engineering. Prof. Levitt is a co-Director of the Computer Security Lab at UC Davis.

Prior to returning to UC Davis, Professor Levitt spent four years at the National Science Foundation during the INCO-Trust project and was involved in the build up of the EU – US collaborations in ICT Trust and Security from the very start.

Professor Levitt's presentation focussed on the motivation from the "U.S. Perspective" to foster international cooperation on security, with a main focus on collaborative data sharing – how to share, what data to share, what guarantees can be made about legal, regulatory, privacy issues, etc.

The many agencies within the US that are involved in cybersecurity were presented and Professor Levitt stressed the point made earlier by Sam Weber of the NSF that a tight integration and harmonization of the agencies involved both on a national and international scale is required. The point was also made that the other stakeholders should also be involved in these efforts, including the companies, research institutions, consultants, and others. The talk focused the two motivational focal points:

1. **A need for highlighting the needs for** a collaborative data sharing framework or architecture to deal with ongoing incidents. This should also not only focus on the technical aspects but should also deal with legal and regulatory challenges. A number of examples were given to show how the attacks don't respect international boundaries and we need to deal with them on a global scale. The systems must be able to monitor data for systems, routers, application logs in which different detailed levels of semantics are needed. There is also the issue of standardization when sharing data in order to ensure protection of data and that policies regarding the protection of data needs are being addressed. Prof. Levitt asserts that these discussions would leads to an architecture and presented some examples (medical data) of how we need to cooperate on an international basis, which is at a very low bandwidth today and this will have to change if we are to get a more favorable balance against the attackers.

2. **The extension of the GENI system to include international components in the future**. GENI is a large testbed in networking including security, which has been in operation for the last 5-6 years, has a primary objective of examining what the future networks will look like at scale. Experiments have been going live across the US to look at this. However, there are plans to have GENI sites internationally and they are looking for participation.

In summary, Professor Levitt said it is viewed as very important from the US perspective to build a framework and architecture for data sharing with collaborative parties from both the EU and further. The incentives are plentiful for this and are highlighted in the presentation materials as the big questions being addressed during the session.

Towards Collaborative Data Sharing – "EU perspective" [14]

Speaker: Barbara Daskala, ENISA, Greece

Barbara Daskala is employed in the European Network and Information Security Agency (ENISA), where she currently works on risk management practices and identifying emerging security and privacy risks posed by new technologies and ways to address them. Before that she was employed in the Institute for Prospective Technological Studies (IPTS) of European Commission's Joint Research Centre, where she was involved in research on the social implications of emerging and future technologies.

Ms. Daskala opened the talk by outlining the role of ENISA. ENISA is an EU agency established in 2004 and is located in Heraklion, Crete in Greece. There are around 65 experts at ENISA and it is an *EU Centre of Expertise specifically* involved in information security that facilitates information exchange across EU institutions, public and private sectors. Therefore, it is quite challenging for ENISA to provide the whole EU perspective on international data exchange needs.

Regarding the motivation for collaboration on data sharing for cybersecurity, ENISA have been involved within INCO-Trust and BIC activities and following the news of all of the recent security breaches, it is quite clear that it is a global challenge and motivation for us to work together to increase levels of security. Furthermore, the different approaches taken in various countries can also complement each other and result in a better methodology for improved security solutions and more effective mitigation.

The challenges we must face together are:

- Different views and mentalities in various countries;
- Different ICT maturity levels in various countries;
- Legal cross-border issues especially when talking about data exchange and sharing;
- For ENISA and EU: different approaches among EU Member States – it is therefore *difficult to have one point of reference!*

Some of the areas that ENISA are engaged in regarding International cooperation include the following:

a) **CERT work.** FIRST is a global initiative for CERTs setting up & incident handling guide, exercise material. Another initiative has been involved in supporting and facilitation of setting up CERTs in eastern African countries, e.g. Kenya, Tanzania.

b) **EU-US Working Group on cyber-security has been recently established in April 2011.** The role is to enhance collaboration between CERTs and facilitate a 1st EU-US cyber security exercise.

Ms. Daskala stressed that this is not an exhaustive list of EU initiatives. Other initiatives undertaken by ENISA include the setting up and running of expert groups of international experts, e.g. in cloud computing, smart phones, life-logging and engagement in "Information exchange" visits: e.g. Japan, Korea, China.

Threats and Actors [15]

Speaker: Sotiris Ioannidis, FORTH, Greece
Sotiris Ioannidis is a researcher with the Institute of Computer Science at the Foundation for Research and Technology (FORTH) in Crete, Greece.

Drawing upon his work in the FP7 projects WOMBAT [16] and SYSSEC [2], Sotiris Ioannidis presented the current situation on threat actors and provided an overview of their capabilities, threat models and assessment of the consequences of breaches or disruptions and their criticality. He stressed that in order to improve our knowledge about malicious code, we must work together on international data exchange especially on malware and to enable increased and better analysis results for context consolidation. This would enable the community to understand malware activities and trends. In order to improve our posture against these threat actors, this work can be supported by technologies and tools developed within these projects including new sensors for data acquisition (wireless, …) and new analysis techniques (code, context, …). The speaker highlighted a number of proposals for new technologies for enterprise and home-use and for new practices (CERTs, ISPs) and regulations.

The speaker focussed on the approach taken by the WOMBAT project, whose goal was the collection of information and alert data from multiple sources to learn something about the attacks. The motivation behind this was to understand the attackers and the enemy as cybercrime has become a huge business. Needed to understand what they were doing by collecting, sharing, manipulating and analysing the collected data. However, it is recognised there are a number of issues when collecting data, including monetary disincentives of sharing data (someone could be looking to make money with it); and of course, privacy issues. WOMBAT pushed for the sharing of this data to give the ability to investigate malware and how the threat actors operate. The first step in the WOMBAT process is data acquisition and collection of the data. The next step was the enhancement of the data to better visualise and contextualise of the data. This enabled more intensive data mining to understand the threats better and allowed the project to then build better tools in a feedback loop. The tools must be dynamic with the services being developed further with more enhancements. The project was able to promote the tools to industry, who were very supportive of the ideas and algorithms and have utilised them into new services. The project strived for a common API that could be adapted by others with different data sources and an interest in examining the data. There has been significant knowledge transfer to the security industry into their security projects and the project has made a great deal of impact and improved the knowledge of malware and threats by looking at the raw data and harvesting of this data via the new tools developed including new sensors used to collect the data.

The speaker concluded with lessons learned within the WOMBAT project. The TRIAGE framework enables multi dimensional analysis of security events. It has been applied to several data sources and led to interesting findings that will improve our ability to counter the many threat actors that are out there. The framework has been used and is being transferred within Symantec. Publications of these lessons contributed significantly to the visibility of WOMBAT, which concluded a few weeks ago.

Straw man architecture for International data exchange and collaborative analysis [17]

> **Speaker:** John C. Mallery, Massachusetts Institute of Technology, Computer Science & Artificial Intelligence Laboratory, Cambridge, MA, United States
> John C. Mallery is a research scientist at the Massachusetts Institute of Technology, Computer Science & Artificial Intelligence Laboratory. He is concerned with cyber policy and has been developing advanced architectural concepts for cybersecurity and transformational computing for the past decade.

John C. Mallery explained that the purpose of this technical part of the session was continuation of the work that was started during an earlier INCO-Trust workshop in May 2010, in New York City, specifically on jointly developing a Secure International Data Exchange Architecture for Cybersecurity outlined by the *Technical Challenges for Transnational Repositories* session[27]. Such a capability would reduce defensive gaps across the contributing states, and build crisis-response capacity and an international system for data exchange related to cyber crime. This would include attack patterns and '*signatures*', best defence practices, and response and recovery – individual and collective. This would greatly improve defensive understanding and coordination resulting in biasing the successful work factors for cyber attack and defense in favor of defenders.

At the workshop in May 2010 and in follow up iterations between the participants, as shown in **Figure 1** [18], a straw-man architecture was generated and this was described in more detail at the BIC session. Due to the duration of the session, it wasn't possible to get into very technical discussions but instead focus on bringing this work to the next level and commitment to the research and development coordination, which will enhance the outcomes through tactical planning, leveraging and combining task-relevant national expertise.

Malicious actors[28] in cyberspace actively exploit the shortcomings in the ability of defenders to coordinate their activities. They can rerun the same attacks against different countries, sectors and organizations so long as cyber data and countermeasures are not being shared effectively.

Mr. Mallery asserted that an architecture for international and cross-sector sharing of cyber threat and attack data will ensure a more effective collective cyber defense than countries, sectors or organizations might otherwise achieve individually.

Figure 1 illustrates an international cyber data sharing architecture that integrate data from multiple countries and sectors and returns collaboratively produce analytical products and threat mitigation techniques. Country fusion centers integrate country information and expertise internationally. Within each country and across its sectors,

[27] Mallery, John C. "Straw Man Architecture for an International Cyber Data Sharing System," position piece, INCO-TRUST Workshop On International Cooperation In Security And Privacy: International Data Exchange with Security and Privacy: Applications, Policy, Technology, and Use, New York: New York Academy of Sciences, May 3 - 5, 2010. http://www.cs.rutgers.edu/~rebecca.wright/INCO-TRUST/position.html

[28] cyber criminals, adversarial national intelligence agencies, hacktivists, and cyber terrorists for starters

shared monitoring infrastructures capture base cyber data at sources. This data is processed to remove personally identifiable information (PII) before being analyzed using shared algorithms to produce results fed back into shared situational awareness. The architecture supports sector-based threat mitigation cycles as well as enterprise information assurance management of value at risk. The architecture supports learning modalities like data refinement to improve data capture, analysis and utility in threat mitigation. Based on knowledge gained about vulnerabilities and attacker vectors, the architecture helps drive improvement of enterprise and infrastructure architectures to improve defensibility.

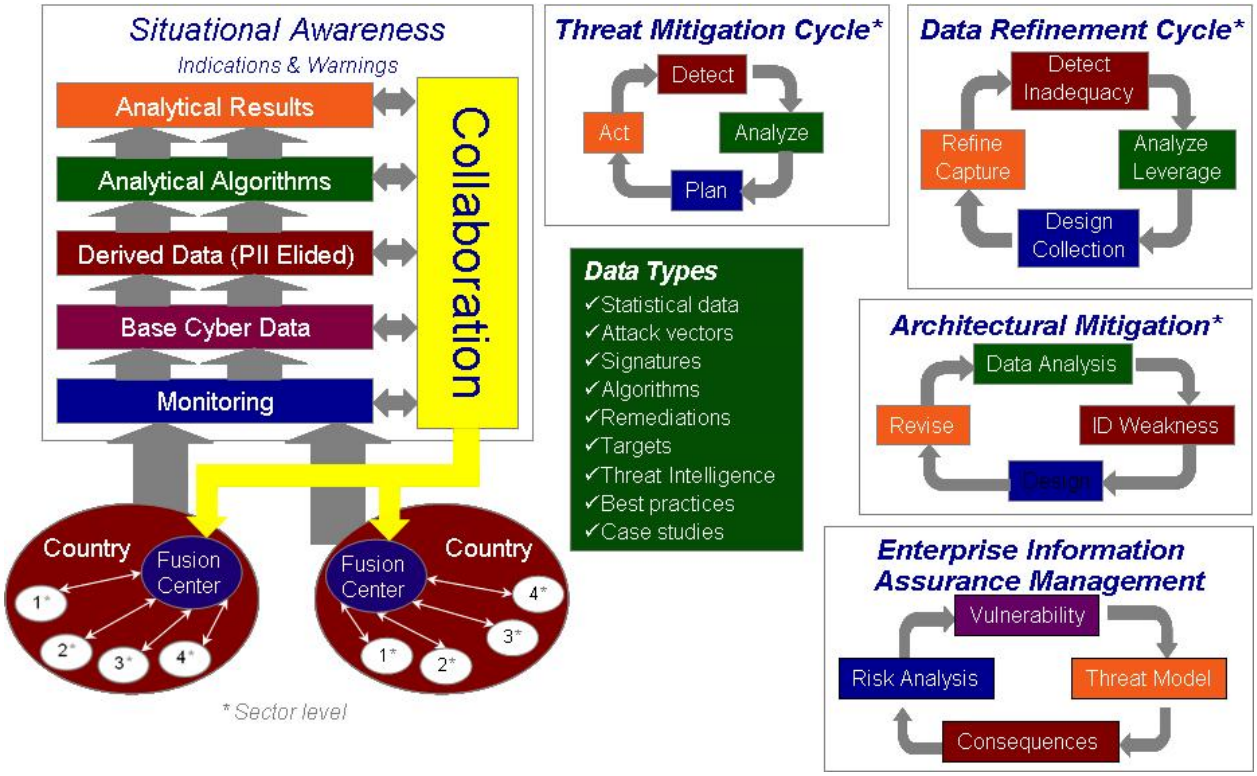

Fig. 1. Straw man architecture for international data sharing and collaboration.

Mr. Mallery explained that this kind of sharing scenario can drive research along many trajectories. The type of data collected needs to be effective and offer leverage for cyber defense. Large-scale analytics over the data need to reveal important patterns in real time and lead to timely threat mitigation. Given an effective sharing architecture, major malicious actors will endeavor to corrupt the data and subvert its operation, and so resilient and trustworthy engineering will be needed for all components from sensors to hosts, monitoring, analysis and mitigation actions. At the same time, PII and enterprise information must be protected to respect important societal values and incentivizing sharing. Difficult technical, legal and administrative challenges in international authentication, authorization, encryption and remote policy enforcement must be overcome to reach higher levels of trust and sharing necessary for weaponizable data like critical infrastructure attacks and mitigations.

Mr. Mallery concluded by emphasising that as an international community, we need to look at optimising the integration of both technical and economic perspectives to favour defensive interventions that disrupt malicious business models.

Figure 2 illustrates the limited scope of conventional technical approaches to cyber defense. By integrating understanding of the attack business model, defenders gain additional opportunities to disrupt the attacker anywhere on his value cycle using passive or active means. Additionally, the resources, capabilities and motivations of the attacker provide constraints on the range of technical defenses necessary for effective defense.

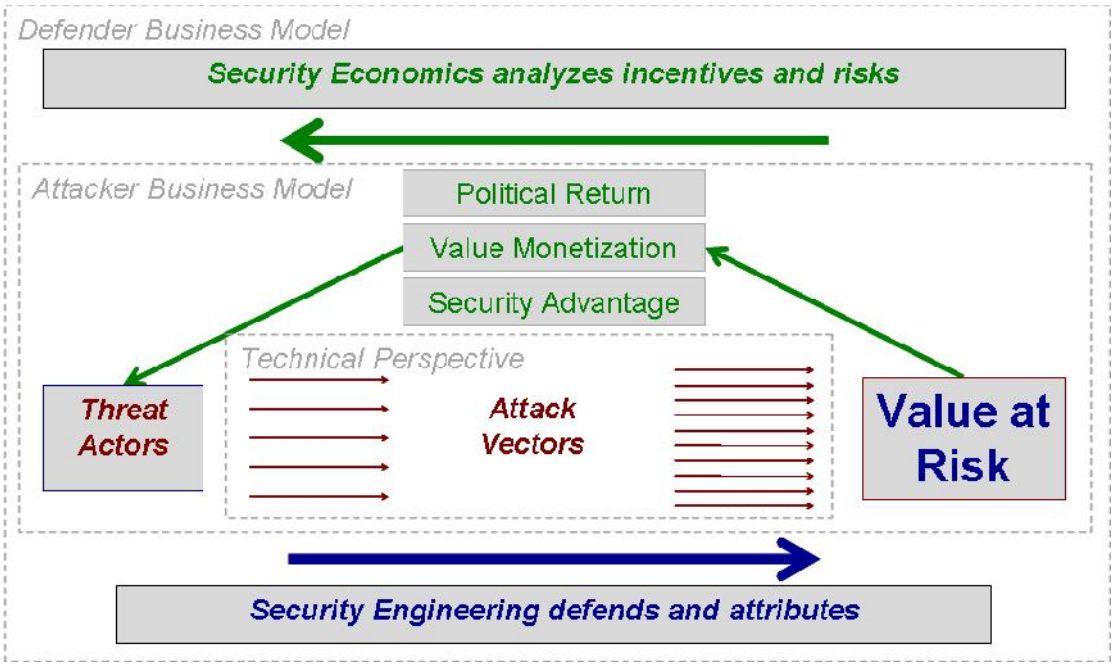

Fig. 2. Optimising integration of technical and economic perspectives for cyber-security.

Data exchange architecture used in a financial application in South Africa [19]

Speaker: Dr Barend Taute, CSIR Meraka Institute, South Africa
Barend Taute is an electrical engineer with a PhD in Electromagnetics. He is employed by the Council for Scientific and Industrial Research in Pretoria, South Africa and his current role is Manager: Contract R&D in their ICT unit. Barend is also FP7 Security NCP for South Africa and involved in various projects that promote Euro-Africa research collaboration.

Dr. Barend Taute set the scene for his talk describing the typical timeline for phishing incidents that have occurred in South Africa as shown in Figure 3. The phisher, the exploited website, the phishing website, the email harvesting activity and the banking victim could all be in different countries, creating various challenges for banks and forensic investigations. The whole process can be conducted with relative ease in a short time-frame using commercially available software.

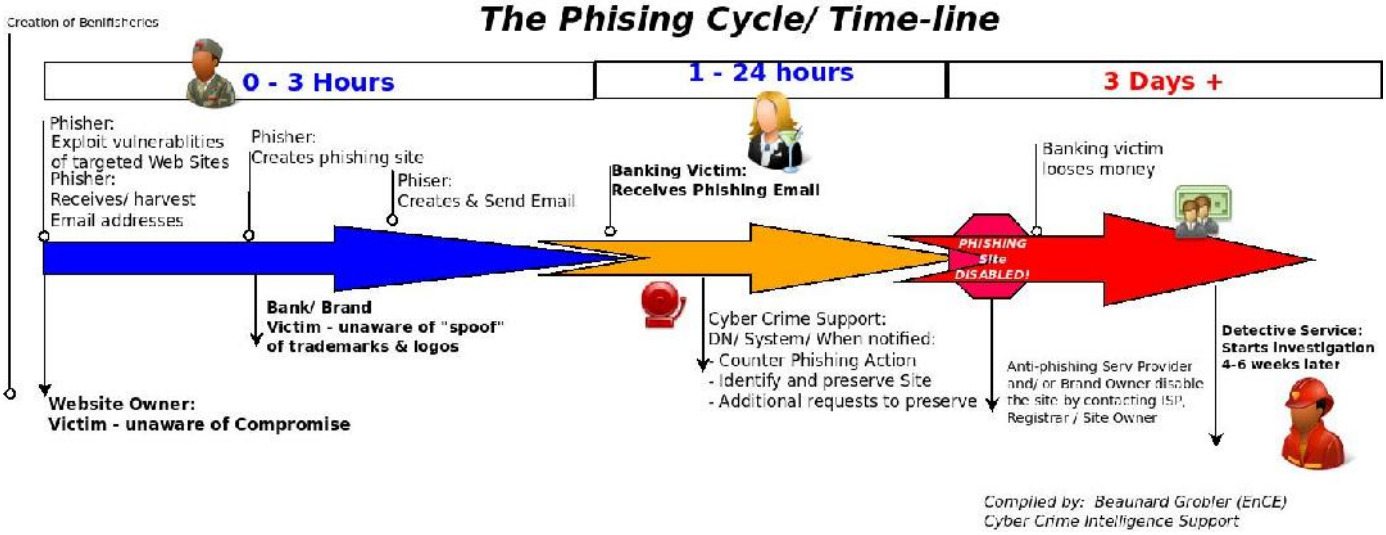

Figure 3. The phishing cycle/time-line.

The challenges for South African researches and investigators include:

- South Africa is getting about 4 % of the world's phishing volume and is currently 4th in the world (down from 18%, 3rd) after USA, UK, India;
- There are still new victims and an increase in local phishers;
- National Computer Security Incident Response Team (CSIRT) is not in place yet.

In addition, a new era of phishing is taking place with the use of malware and spyware, which enables the criminals to be more creative in their targeting of victims while remaining less visible. The steps to combat phishing are different for police and banks: Banks want to close down the phishing activities (via service providers) as soon

as possible, while the Police need to investigate and find forensic evidence on active sites. This requires mutual legal assistance with the countries in question (not always in place) and gets complicated due to privacy issues and/or the lack of a local victim or complainant.

In order to address these challenges, Dr. Taute explained that trust must form the basis for international intelligence sharing and quick International Cyber Legal Assistance when it is needed. In addition, cyber security awareness is needed for users at all levels. This level of awareness is quite difficult in the developing world due to the lower levels of ICT literacy, and moving in a short time from very low levels of communications to full broadband connectivity. This makes them both more vulnerable and potentially becoming the hosts for cyber attacks. We need to look at creative ways to raise awareness so that the message is retained, e.g. using games and videos.

Dr. Taute pointed out there is a research project on network attack prediction and visualization using network telescopes to examine attack taxonomy and provision of alerts and data sharing.

Dr. Taute concluded by referring to a sector level data sharing architecture for the financial sector in South Africa, involving 6 major banks with internet banking that use techniques such as one-time passwords to cellphones. This is coordinated by the SA Banking Risk Information Centre. They are already gathering and sharing crime related information for the banks. There is a banking CSIRT in the planning phase and the data sharing architecture has some challenges concerning privacy and reputational risk that must be addressed firstly within the sector and then it will be addressed with local internet service providers and eventually international banks.

Identity related issues for data handling and aggregation [20]

Speaker: Glenn Gran, International Organisation for Knowledge Economy and Enterprise Development (IKED) –Sweden. Glenn Gran is a programme manager at IKED, the coordinator of the FP7 GINI Support action Project. Glenn Gran is an expert on innovation and ICT policies. Prior to this, he was the Research Director in an organisation affiliated with IKED, the Global Trust Center. Here he developed special competences in outstanding issues in the development and implementation of radical new solutions to improved ICT and cloud computing governance.

In his presentation, Mr Gran provided an overview of the GINI-SA project, which aims to investigate and establish the foundations for the architectural, legal, regulatory requirements, as well as the provisioning and privacy enhancing aspects, of an environment of user-centric identity management services. GINI-SA is based on the assumption that individuals, i.e. citizens, consumers, users of any related services, should be able to manage their own identity data and provide it in an open and flexible manner.

On this basis, the user can create and manage its own Individual Digital Identity (INDI) throughout its lifecycle (creation, change, management, revocation etc.). To enable trust between the actors in the INDI environment (INDI Users, Operators, Data Sources and Relying Parties), GINI envisions an operator-based trust model (i.e. 'brokered' trust relationship), where multiple INDI Operators mediate trust among the different actors involved. One of the underlying objectives of the GINI conceptual model is to remove (or at least minimize) the need for bilateral negotiation and/or communication among the different actors when making use of INDI Services. The INDI Operator with whom the INDI User has a direct contractual relationship serves as the main point of entry to the INDI environment for that User. One of the key benefits of the Operator Network model is that it can be standardised and regulated easier than a model, which is based on very heterogeneous and uneven entities, and this can greatly enhance the user's ability to build trust relationships with Operators.

Mr. Gran highlighted the fact that the INDI is verifiable against authoritative registers or data sources that the user selects. In principle, the INDI can be verified in two different ways: the user submits data to the Operator and these are verified against data sources of the users choice or the user does not submit data to the Operator but points to the data source where the data is located, and registers verified (and verifiable) links to those data. Obviously the latter is preferable from a privacy point of view since it removes the need to disclose the identity and send new data to the operator.

Mr. Gran also emphasized that using authoritative registers or data sources for verification will allow developers to leverage existing infrastructures, and offers the advantage of having single points of contact to update and manage information. This may help reduce the amount of copies of the same information in different databases, among which discrepancies may start to develop over time. From a privacy point of view, reliance upon distributed information repositories may additionally help minimize the amount of data stored centrally, which may in turn reduce the potential gain for attackers and as a result reduce cyber crime. However, the actual benefits for data protection and privacy will depend largely on the implementation model and the safeguards that are put in place.

The GINI-SA recently finished the first year of the project, and will in the coming year put strong attention on the issue of the business model and what is required for developing viable operator solutions based on paying customers.

Legal Issues Associated With Data Collection & Sharing [21]

Speaker: Jody R. Westby, Esq., Global Cyber Risk LLC
Jody R. Westby is CEO of Global Cyber Risk LLC, located in Washington, DC. Ms. Westby also serves as Adjunct Distinguished Fellow to Carnegie Mellon CyLab. She chairs the American Bar Association's Privacy & Computer Crime Committee (Section of Science & Technology Law) and co-chairs the World Federation of Scientists' Permanent Monitoring Panel on Information Security. She is the author of the *Legal & Policy Tool Chest for Cyber Security R&D* and the *Legal Guide to Cyber Security Research on Botnets.* She has published four books on international issues pertaining to privacy, cybercrime, cyber security and enterprise security programs, as well as numerous articles and papers. She speaks globally on these topics.

Ms. Westby described the problem areas that arise from the complex legal and regulatory situations when dealing with data collection and the sharing of this data for for the purposes of cybersecurity research and development (R&D). As cyber attacks become more complex, organizations also are becoming more concerned about the legal and policy considerations associated with R&D projects, particularly those involving botnets or sophisticated attack structures, because they can raise a number of legal issues. Guidance on the legal, regulatory and privacy issues, however, is scarce and highly complicated. This complexity is compounded by a highly inconsistent global legal framework that makes an analysis of the legality of a research approach even more difficult.

In order to improve the situation, the Department of Homeland Security's Cyber Security R&D Division funded a project entitled "New Frameworks for Detecting and Minimizing Information Leakage in Anonymized Network Data." Within this project, a publication was developed by Ms. Westby entitled The *Legal & Policy Tool Chest for Cyber Security R&D* (*Tool Chest*). Ms. Westby described the Legal & Policy Analysis Tool Chest, which is a comprehensive set of three tools that may be used both to help analyze the legal and policy implications associated with the use of traffic data in cyber security R&D and to mitigate identified risks. The tools are:

1. Legal Analysis Tool on Obtaining & Using Network Communications Data (Legal Analysis Tool), which focuses on obtaining, using, and disclosing intercepted and stored communications data.
2. Privacy Tool on Using Network Communications Data (Privacy Tool), which focuses on the relevant privacy legal considerations with this data.
3. Protection Measures Tool, which contains sample contract clauses and memoranda of agreement that can be used by researchers and their organizations to mitigate legal risk.

While the Tool Chest is based on U.S. laws, Ms. Westby stressed that it also takes into account foreign legal issues, such as disparities in privacy laws, especially with respect to the EU. The Privacy Analysis Tool explains these legal and policy privacy considerations and provides a decisional framework to guide researchers and institutional review boards (IRBs) through the process of determining (1) whether a dataset has legal or privacy issues associated with it, (2) whether these issues are fatal and may preclude the use of the data, and (3) whether certain legal issues may be mitigated or eliminated through anonymization or other de-identification techniques.

Ms. Westby presented the *Legal Guide on Cyber Security Research on Botnets (Botnet Legal Guide),* which was developed in order to extend the *Tool Chest's* analysis and examine the myriad of legal issues associated with this particular type of research. The *Botnet Legal Guide* also was funded by DHS's Cyber Security R&D Division and developed by Ms. Westby as a component of a technical research project led by Georgia Institute of Technology on "Countering Botnets: Anomaly-Based Detection, Comprehensive Analysis, and Efficient Mitigation."

In conclusion, the *Tool Chest* and *Botnet Legal Guide* are companion publications that provide the cyber security research community with a central repository of definitions, descriptions of the laws, worksheets, decisional frameworks, tables simplifying privacy provisions and penalties, and conclusions regarding how U.S. laws apply to datasets to be used in research projects and impact research activities. International considerations, especially with respect to privacy and cybercrime laws, present challenges for researchers that require careful and joint analysis. The *Tool Chest* and *Botnet Legal Guide* offer a positive step toward helping researchers, IRBs, legal counsel and management better understand the legal issues associated with research projects and the data used in them. Both publications are being published by the American Bar Association in the fall of 2011.

Ms. Westby stressed the need for international collaboration between the legal and technical communities, particularly with respect to exploring the extraterritorial reach of laws and inconsistencies in legal frameworks. Researchers particularly need to better understand critical jurisdictional differences in the global legal framework for interception, privacy, and cybercrime. Programs such as PREDICT[29] that include the legal analysis of datasets that are offered to researchers help build confidence that data used in research efforts will not run afoul of the law, but they do not address the legality of the activities undertaken by researchers when using the data. The development of best practices with respect to certain research activities would make a significant difference toward encouraging legal conduct in R&D projects.

More information on this work can be found in a recently published paper by Ms. Westby in the proceedings of the Building Analysis Datasets and Gathering Experience Returns for Security (BADGERS) 2011 Workshop, Apr. 10, 2011, Salzburg, Austria (part of EuroSys 2011), http://iseclab.org/badgers2011/.

[29] PREDICT is an acronym for the Protected Repository for the Defense of Infrastructure Against Cyber Threats sponsored by the U.S. Department of Homeland Security (DHS) Science & Technology Directorate's Cyber Security R&D division,

SUMMARY AND CONCLUSIONS

The goals of the BIC session were the following:

- *Planning matters:* to prepare the ground for the extended BIC Annual forum workshop currently scheduled for late 2011;
- *Scope and topics for collaboration:* to clarify scope and possibilities for international collaboration on ICT trust and security; as an example of identified topics, to continue the work on the development of a *straw-man* architecture for secure international data exchange for cybersecurity, introduced at an earlier (May, 2010) INCO-Trust workshop, and to explore the technical and organisational challenges and constraints that arise from this.

A further goal was to benefit from co-locating this meeting as part of the SysSec Workshop to allow contribution by a wide representation from security research communities.

The results of the meeting are summarised against these headings.

Planning matters

The precise date and location for the BIC annual forum in Q4 2011 is still under discussion as many of the stakeholders need to be included in the discussions. Among the options considered is to relate it to another large scale event being held in the EU during Q4 2011.

The mission of the BIC annual forum is discussion and agreement on technological challenges/gaps of common interest amongst the countries, agree on what can and needs to be done internationally (who can contribute to what), and then work at an international level towards delivering on cooperation towards solving these joint technological challenges. The forum will enable the working towards the definition of tangible international activities, including establishing success metrics and setting up global projects.

The objectives of the BIC annual forum are the following:

- Identification of the technological challenges that really need and could be tackled in common between the countries so they can be elaborated clearly with the policy makers in the respective countries as a way forward;
- highlighting the current bi-lateral (and potentially overlapping) country to country cooperation(s) into a more comprehensive unified global cooperation eg. US-India, EU- US, etc.
- Identification of the responsible agency(ies) per country and points of contacts to participate in the global cooperation on ICT trust and security.

In the BIC session on 6th July 2011, during discussions and presentations, a number of topics were already identified for further planning consideration that can be carried forward to a longer, more detailed session at the BIC annual forum. Contributions were invited on these in preparation for the larger event. These include:

- What kind of data sharing and collaborative analysis architecture could be built

with today's technologies and operational knowledge?

- Who are the current actors around the globe and what are their approaches and can these be leveraged and harmonized together?
- What are the gaps?
- What research would be needed to build a better data exchange architecture for cyber security in the 5-10 year time frame?
- Who are the actors needed to carry out this research and where are they from?
- What organizational modes are necessary for this research to proceed most expeditiously?
- What funding sources and mechanisms can be mobilized to support the joint international efforts required in research and adoption?
- In order to better motivate countries to contribute and support the effort, we should highlight the rationale and motivation for designing and building sophisticated architectures for international cyber data sharing, collaborative analysis, and collective defence. For example,
  - Dramatically improve defensive coordination to move the economic advantage away from offence in favour of defence;
  - Create shared real-time situational awareness;
  - Identify cyber data for sharing together with leverage scenarios and collection issues;
  - Motivate targeted research to enable effective collection, sharing, analysis and response.

Scope and topics for collaboration

During the session on 6th July 2011, although there wasn't sufficient time to allow for more in-depth exploration or further detailing of the proposal for a data-sharing framework, it was clear that this provided a powerful example of where well-organised and motivated international collaboration could provide the leverage to address high-priority issues: in this case, rapid, collective response to attack or failure in cyberspace, through the sharing of intelligence and the design and development of shared defence strategies. As with all defences, penetration by an attacker would have drastic consequences, so the protection of the system itself and of its contents leads to further challenges.

A number of technical aspects were highlighted when going through the straw-man architecture for coverage at the larger workshop being planned for Q4 2011. These included:

- ***Research required on technical enablers:*** The enablers for a secure international data exchange architecture eg. cryptography based obfuscation, sensors on the network, monitoring traffic capabilities, privacy protecting identity management, amongst others.
- ***Integration of technical and economic perspectives:*** *to* optimize defensive interventions for the disruption of malicious business models.

- ***Sharing Incentives:*** Research is needed on incentivizing data sharing and collaboration across entities, sectors and countries. Basics of how we share recognizable data, especially on critical infrastructures and across different countries. eg. share patterns for recognizing advanced persistent threats without losing efficacy if they are exposed. What obfuscation and security measures would make patterns easier to share?
- ***Collection Prioritization:*** Methodologies are needed for identifying and prioritizing data for collection in order to yield high leverage against cyber threats across different time.
- ***Learning and Agility:*** Data sharing and collaboration needs to evolve rapidly to keep pace with emerging threats.
- ***Resilient Sharing Architecture:*** Research needs to produce a defensible architecture for sharing and collaboration.
- ***Integration of technical and legal requirements:*** The need for international collaboration between the legal and technical communities, particularly with respect to exploring the extraterritorial agreements, including Safe Harbor agreements, pertaining to reach of laws and inconsistencies in legal frameworks.
- ***Trust:*** Data sharing and collaboration will only be a good as the confidence participants have in the ability of the architecture to enforce access control and dissemination policies.

Acknowledgments

The BIC project is funded under Call 5 of FP7 ICT and began on 1st January 2011 with a duration of three years. The project is supported by the European Commission DG INFSO, Unit F5 ICT Trust and Security Research [22].

The BIC project would like to acknowledge the support of the organizing committee members and to the SysSec project workshop organizers.

A number of additional positions were submitted to the organisers prior to the session and there wasn't enough time to include during the session. Please see [23], [24], [25], [26] for more details. The presentations are available at http://www.bic-trust.eu/events/event/bic-session-syssec-workshop/.

REFERENCES

[1] BiC project web site http://www.bic-trust.eu/

[2] SysSec project web site http://www.syssec-project.eu/

[3] http://www.cs.rutgers.edu/~rebecca.wright/INCO-TRUST

[4] http://www.securityconference.de/Home.4.0.html?&L=1

[5] https://update.cabinetoffice.gov.uk/sites/default/files/resources/CyberCommunique-Final.pdf

[6] http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CL=ENG

[7] Remarks at the 28th Annual International Workshop on Global Security, Paris, France 16th June 2011 http://www.defense.gov/speeches/speech.aspx?speechid=1586

[8] International cooperation "at nascent stage" - U.S. Secretary of Homeland Security Janet Napolitano, Vienna, 1st July 2011. http://www.reuters.com/article/2011/07/01/us-cybercrime-idUKLDE75T1CC20110701

[9] http://www.syssec-project.eu/media/page-media/23/bic2011-01-clarke.pdf

[10] SysSec workshop http://www.syssec-project.eu/events/1st-syssec-workshop-program/

[11] Clarke, James, Wright, Rebecca, et al., "D4.2 INCO-Trust 2nd Workshop report", available at http://www.inco-trust.eu/incotrust/general/project-impact.html

[12] http://www.syssec-project.eu/media/page-media/23/bic2011-02-weber.pdf

[13] http://www.syssec-project.eu/media/page-media/23/bic2011-03-levitt.pdf

[14] http://www.syssec-project.eu/media/page-media/23/bic2011-04-daskala.pdf

[15] http://www.syssec-project.eu/media/page-media/23/bic2011-05-ioannidis.pdf

[16] WOMBAT project web site http://www.wombat-project.eu/

[17] http://www.syssec-project.eu/media/page-media/23/bic2011-06-mallery.pdf

[18] Mallery, John C. "Straw Man Architecture for an International Cyber Data Sharing System," position piece, *INCO-TRUST Workshop On International Cooperation In Security And Privacy: International Data Exchange with Security and Privacy: Applications, Policy, Technology, and Use*, New York: New York Academy of Sciences, May 3 - 5, 2010. http://www.cs.rutgers.edu/~rebecca.wright/INCO-TRUST/position.html

[19] http://www.syssec-project.eu/media/page-media/23/bic2011-07-taute.pdf

[20] http://www.syssec-project.eu/media/page-media/23/bic2011-08-grann.pdf

[21] http://www.syssec-project.eu/media/page-media/23/bic2011-09-westby.pdf

[22] DG INFSO Unit F5 web site http://cordis.europa.eu/fp7/ict/security/

[23] Challenges in streaming temporal and spatial network data (78.1 KB) Chalmers University

[24] Multi-party computation approach as a privacy solution developed in the SEPIA project (314.5 KB) ETH Zurich

[25] Different approaches for data sharing (78.0 KB) Moscow State University

[26] Joint collaboration to guarantee an optimal incident response and post incident data analysis in mobile scenarios (148.2 KB) JRC & KTH

Annex IV. BIC International Advisory Group (IAG) Inaugural meeting minutes

BIC International Advisory Group (IAG)
Inaugural meeting
29th November 2011
Brussels, Belgium
Meeting Minutes

Introductions & welcome

Present

Priscila Solis Barreto	University of Brasilia, Brazil
Jan Eloff	SAP Meraka UTD & University of Pretoria, South Africa;
Abhishek Sharma	NetEdge Tele-Solutions (NTS); India
Hiroyuki Hishinuma	National Institute of Information and Communications Technology (NICT), Director of Europe Center, France
Gary Morgan	Commonwealth Scientific and Industrial Research Organisation (CSIRO); Australia
John C. Mallery,	Massachusetts Institute of Technology; USA
Jim Clarke	Waterford Institute of Technology (BIC)
Keith Howker	Waterford Institute of Technology (BIC)
Michel Riguidel	Telecom Paris-Tech, ENST, France (BIC)

Apologies

Sam Weber	National Science Foundation; USA
Karl Levitt	University of California, Davis, USA
Pamela Moss,	Natural Sciences and Engineering Research Council of Canada (NSERC). Canada
Yasutaka Sakurai	Japan Science and Technology Agency (JST),
Young Tae Cha,	Ministry of Knowledge Economy (MKE); Korea
Souhwan Jung,	Soongsil University
Heung Youl Youm	Soonchunhyang (SCH) University
Neeraj Suri	TU Darmstadt (BIC)
Aljosa Pasic	AToS (BIC)
Jesús Villasante	European Commission, Head of Unit F5, Trust and Security
Cristian Olimid	European Commission, BIC project officer.

Round table of participants

Priscila Solis Barreto is a Professor at the University of Brasilia in Brazil. Professor Barreto was involved during the last joint Brazil – EU call and worked very closely with CNPq[30] and MCT (Ministry of Science and Technology) in the realisation of the Joint call. Professor Barreto played a pivotal role during the setting up of the Joint call and was in charge of the specific topic on Future Internet, which included Trust and security in the final version of the call. Prof. Barreto continues to have close ties with the international cooperation departments within the Brazil government in both CNPQ - INCO unit and MCT and is the research representative of them on the BIC IAG.

Jan Eloff is currently appointed as Research Director at SAP Meraka UTD / SAP Research Pretoria and as an Extraordinary Professor in Computer Science at the University of Pretoria. At the University of Pretoria, he is a co-founder of the Information and Computer Security Architectures (ICSA) research laboratory. He represented South Africa as an expert member on IFIP Technical Committee 11 (Information Security). Along with Barend Taute, he is especially appointed a research member of the BIC IAG by the Department of Science and Technology of the government of South Africa.

[30] The National Council for Scientific and Technological Development (CNPq) http://www.cnpq.br/english/cnpq/index.htm

Abhishek Sharma is Co-founder, MD & CEO of NetEdge Tele-Solutions (NTS). He is a veteran of the ICT domain with authority on Telecom & Radar. Abhishek has a B.E. Degree in Electronics & Telecom Engineering, from GEC, Jabalpur, M.E. in Computer Sc & Automation from I.I.Sc, Bangalore, Masters in Management Studies from College of Defense Mgmt & M.B.A. in Marketing from IGNOU Delhi. His company develops mobile applications on Utility VAS for GSM/ CDMA mobile users. Abhishek is also international consultant on Mobile VAS, Telecom Network, Radar Data Systems and Avionics. He has rich experience of managing large business, Operations & projects, setting up GSM, CDMA, Satellite & Radar NW and BSS, OSS solutions. Abhishek has participated in many national 7 international seminars and events and has pitched novel product & solution ideas. Mr. Sharma was invited to give the IAG a short presentation on the funding structures of the India government in areas related to trust and security.

Hiroyuki Hishinuma is currently Director of Europe Center, National Institute of Information and Communications Technology (NICT), which is a research institute of ICT in Japan. Before he came to NICT, Mr. Hishinuma worked in the Ministry of Internal Affairs and Communications (MIC), the Government of Japan, dealing with telecommunications policy. Mr. Hishinuma was invited to give the IAG a short presentation on the funding structures of the Japanese government in areas related to trust and security.

Gary Morgan is Director Business and International, Digital Productivity at the CSIRO ICT Centre. The ICT Centre is the CSIRO's hub for innovative information and communication technologies research applied across the breadth of CSIRO's engagement with industry and society. In this role, Gary is responsible for Business Development in the Digital Productivity Portfolio themes including Health Services, Smart Infrastructure Services, Government and Commercial Services, and Advanced Broadband Networks & Services. Gary is also responsible for the International engagement strategy of the ICT Centre. The Australian Government are in the process of considering nomination of the CSIRO ICT Centre to become the National Contact Point for Europeans connecting with ICT in Australia.

John C. Mallery is a research scientist at the Massachusetts Institute of Technology, Computer Science & Artificial Intelligence Laboratory. He is concerned with cyber policy and has been developing advanced architectural concepts for cybersecurity and transformational computing for the past decade. He was actively involved in the INCO-Trust project as well as BIC. He is a research representative of the BIC IAG.

James Clarke is Project Coordinator of the BIC project, which stands for Building International Cooperation for Trustworthy ICT: Security, Privacy and Trust in Global Networks & Services. BIC will engage the European Union trust and program management (funding organizations) and research communities with their peers in Brazil, India and South Africa and enable the collaboration with research communities in trust and security already established in the US, Australia, Japan, Korea and Canada established in the recently concluded INCO-Trust project that Mr. Clarke also coordinated from 2008 - 2010. In addition, Mr. Clarke is actively involved in the research community, having served in various international conference committees as organizing, technical and program committee member.

Keith Howker has more than fifty years experience in ICT, having joined the Manchester University ATLAS team on graduating in mathematics in 1959. He has been active in promoting trust and security work in international standards and the framework programme since the 1980s. Following retirement from Fujitsu/ICL, where he established and managed the RACE project *SESAME*, he worked for the EC in the then DG XIII on the planning of IST security aspects of FP4. He has since contributed to several security-related projects for Royal Holloway University of London, K U Leuven and Vodafone – *ASPeCT, USECA, NESSIE, SHAMAN, PAMPAS,* and *Ambient Networks,* where he led the security cross-issue work. He was closely involved in establishing the SecurIST, Think-Trust and Effectplus projects and in working with the Advisory/steering Boards related to these projects. Within the BIC project, Mr. Howker will be assisting Mr. Clarke with the running of the BIC IAG.

Michel Riguidel is Professor Emeritus, and previously the Head of the Department of Computer Science and Networks, at Telecom ParisTech (École Nationale Supérieure des Télé-communications, 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 is contributing to the Coordinated Action in international security research of the FP7 BIC (2011-2013) and caretaker for security and trust of the FIA (Future Internet Assembly). He has several patents in security (firewall, watermarking and protecting CD ROM, illicit content downloading).

Jim Clarke gave an overview of the situation relating to the countries that were not able to attend the first IAG meeting.

BIC countries	**Overview**
India	In August, 2011, the project had a meeting at DIT with Dr. N.Vijayaditya, Controller of Certifying Authorities[31], one of the DIT units funding security aspects.. However, it was recommended to meet other DIT officials and Mr. Sharma had committed to helping us meet these officials in December 2011 during a BIC mission to India. These DIT officials are: Dr. Gulshan Rai, Director General, Government of India, Ministry of Communication & IT, Department of Information Technology (DIT), STQC Directorate and Mr. Rajneesh Agrawal, Director, Government of India, Ministry of Communication & IT, Department of Information Technology (DIT), International Cooperation & Industrial Promotion. Bilateral Trade Division.
INCO-Trust countries	**Status**
U.S.	Karl Levitt of University of California, Davis had planned to attend but was not able due to a sudden illness that prevented him from flying. Regarding NSF participation, it is a bit unclear who will continue after Carl Landwehr's departure from the NSF. Although originally scheduled to attend the annual forum and BIC IAG meeting, Sam Weber of the NSF was not able to attend due to a sudden scheduling conflict.
Canada	Pamela Moss, Director/Directrice, Manufacturing, Communications and Technologies, Research Partnerships Programs, Natural Sciences and Engineering Research Council (NSERC) of Canada. Dr. Moss was actively involved in the organisation of the Canada - EU (DG INFSO) workshop on held in Canada during March 2011. Subsequently, had an audio conference meeting with the BIC coordinator explaining the various funding mechanisms in Canada related to ICT. The NSERC has funded a Strategic Research Network known as ISSNet https://www.issnet.ca/about-issnet, whose primary focus is computer and network security emphasizing computer systems research, with an experimental or observational approach. Dr. Moss is interested to participate but is waiting on final approval as to the priority areas for NSERC.
Japan	Mr. Yasutaka Sakurai, recently became the new BIC contact within Japan Science and Technology Agency (JST), International Affairs department. Mr. Sakurai was unable to attend due to other commitments.
Korea	There are three committed IAG members: Dr. Young Tae Cha, Program director for Ministry of Knowledge Economy (MKE) in the security area; Prof. Dr. Souhwan Jung, Professor, School of Electronic Engineering, Soongsil University; and Prof. Dr. Heung Youl Youm, Professor Soonchunhyang (SCH) University, Korea. All three sent apologies as they had prior commitments and could not attend.

[31] http://www.mit.gov.in/content/controller-certifying-authorities-cca

Special Invited talks from researchers in India and Japan

Abhishek Sharma on ICT trust and security RTD in India:

Mr. Sharma gave an overview of the funding mechanisms in India. The main funding agency responsible for funding Research and Technological Development (RTD) is the Department of Information Technology (DIT)[32], which falls within the Ministry of Communications & Information Technology of the Government of India. There are a number of units in DIT dealing with areas related to ICT trust and security, the closest of which would be the Cyber Security R&D department [33] . Mr. Sharma explained the processes for getting to meet the government respresentatives and he committed to assisting the BIC project in making contact with right personnel in DIT during their visit during December 2011.

Hiroyuki Hishinuma on ICT trust and security RTD Japan:

Mr. Hishinuma outlined the role of the Ministry of Internal Affairs and Communications (MIC)[34] in funding technological research in Japan and told how there was an EU – Japan Information day held on 19th October 2011 in which there was a specific topic related to ICT trust and security. Mr. Clarke was present at that event and presented the EU work on network and information security and privacy and how there could be opportunities for joint research on these topics between the two countries. In addition, there are discussions ongoing about the potential of a joint call between Japan and the EU possibly in 2013. Mr. Hishinuma was unsure of the best contact point within MIC for contacting related to the BIC IAG but committed to finding out.

IAG Terms of reference

The terms of reference of the IAG were discussed and no issues were raised (Appendix 1). The main expectations of the IAG members are the following:

- To facilitate collaborations between your national ICT Trust and Security constituencies and related ICT trust and security related constituencies from other countries; The IAG will be the forum bringing together the countries representatives from the earlier INCO-Trust participants and the BIC countries;
- To review the situation on International collaboration strategy in ICT trust and security on a regular basis providing advice on the priorities for international cooperation between the respective research communities, providing directions to the project and recommendations for improvement;
- Assist in the building of the working groups to enable BIC to structure relationships and linkages and facilitate contacts for theme based workshops or other networking events;
- Assisting the project in building a longer term strategy for cooperation that would go beyond the life of the project.

Discussion with members on the structure and suggestion for additional members

The IAG members were in agreement with the current structure of keeping the IAG membership low in numbers with IAG members of a stature that could bring the important messages to the policy and decision makers back home and strongly push for them to support the ongoing work of the project.

A number of suggestions were made on additional member types e.g. members from Standards bodies and other dissemination channels. It was suggested that perhaps this would not be

[32] http://www.mit.gov.in/content/about-dit
[33] http://www.mit.gov.in/content/cyber-security-strategy
[34] http://www.soumu.go.jp/english/eo.html

appropriate due to the nature of the message that we are trying to bring across to the policy and decision makers as participants to RTD projects that would be set up within Joint calls. Having members outside this scope might cause some confusion on the message. However, this would be checked with the European Commission to check on their views.

Review of the Annual Forum

The IAG members were unanimous in their approval of the BIC annual forum result as to the level of the organisation and content within the Forum.

Although there was a decent coverage from EU-Asia-Pac regions, it was suggested that for the next event, an attempt should be made to attract more participants from around the globe. The positioning of the event next to other relevant events is a very good idea to accomplish this. The IAG members committed to helping locate such events in the latter half of 2012. A member asked if it was possible to hold an Annual forum outside of Europe. This would need to be checked as it is currently supposed to only occur within the Europe but perhaps if there was an extraordinary reason for this, it may be possible.

Agree Way forward

Jim Clarke presented the BIC timeline to highlight the objectives for year 2:

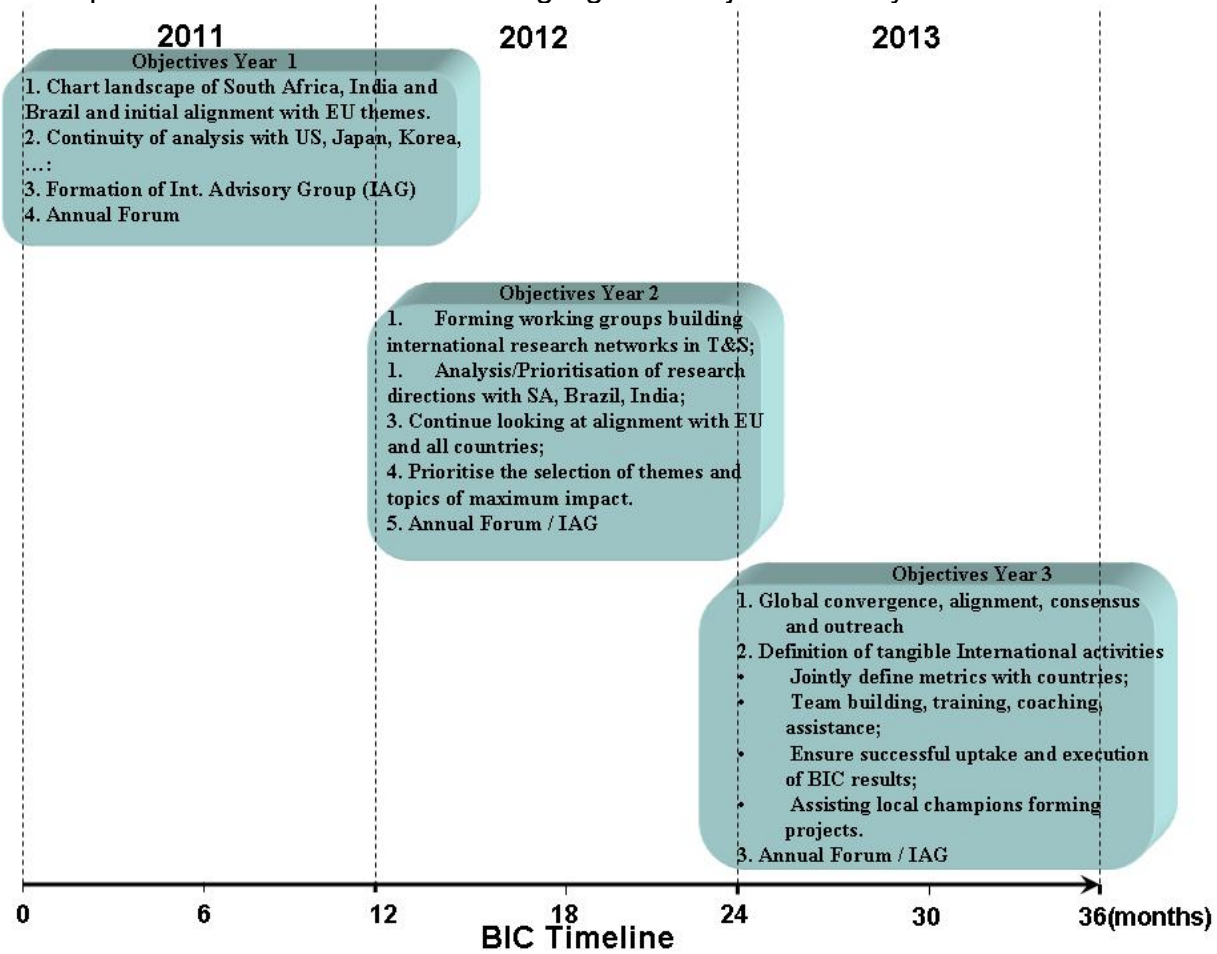

Figure 1. Timing of Objectives over project life-cycle.

Any other business

On behalf of the IAG, Jim Clarke thanked the European Commission for their kind offer to host the BIC IAG meeting at their premises on the morning of 30Th November if needed.

Notes written by Jim Clarke, BIC Project coordinator and Keith Howker, WIT-TSSG.

Appendix 1. Invitation letter and IAG Terms of Reference

OFFICIAL INVITATION AND TERMS OF REFERENCE TO THE INAUGURAL BIC INTERNATIONAL ADVISORY GROUP (IAG) MEETING.

For attention of: BIC International Advisory Group (IAG) members who are available to attend the BIC Annual Forum on 29th November 2011 (distribution list below)

Dear IAG Members, Date: 28th November 2011

Subject: Invitation to the BIC International Advisory Group (IAG) meeting, 29th Nov. 2011.

On behalf of the BIC project, I would like to invite you to the inaugural meeting of the BIC International Advisory Group (IAG). I would like to acknowledge that the European Commission had kindly offered to host the IAG meeting at their premises on the morning of 30Th November but after discussing with some of you and carefully examining the possibilities, in order to enable participants to take part in the EURASIAPAC workshop on 30th November and for greater flexibility with travel arrangements, the IAG meeting will take place immediately after the BIC Annual forum on 29th November 2011 at 17:30hrs (5:30pm).

The venue of the IAG meeting is the same as the BIC Annual forum at the Radisson Blu Royal hotel. I will advise later on the exact room number at the hotel as it will be allocated a smaller room. The meeting will start at 5:30pm and will last a maximum of 2 hours with the following agenda:

a. Roundtable of participants and short presentation on members who couldn't attend by Jim Clarke;
b, Special invited talks from researchers from India and Japan attending the BIC Annual forum to explain the structure of research funding mechanisms in their trust and security / INCO areas;
c. IAG terms of reference (see next page);
d. Discussion with members on structure of IAG;
e. Suggestions for additional members of IAG;
f. Review of the annual forum including challenges, topics and approach for long term strategy on international cooperation in trustworthy ICT;
g. Agree way forward;
h. Any other business.

Note: As we will have such a long day already at the annual forum, and since you are probably already travelling, it isn't necessary to use presentation slides during the IAG meeting unless you would prefer it.

If you need any further information, please do not hesitate to contact me or discuss with me in person during the BIC Annual forum on Tuesday. We look forward to seeing you.

Yours Sincerely,

James Clarke

BIC Project Coordinator
Waterford Institute of Technology
TSSG - Science and Technology Board Member
Cork Road
Waterford
Ireland

jclarke@tssg.org
http://www.tssg.org/
Tel. +353 71 9166628 Mob. +353 87 2323931

IAG Distribution list: Priscila Solis Barreto, Univ. Brasilia, Jan Eloff, SAP Meraka UTD & University of Pretoria, South Africa; Gary Morgan, Commonwealth Scientific and Industrial Research Organisation (CSIRO); Karl Levitt, University of California, Davis; John C. Mallery, Massachusetts Institute of Technology; BIC members: Michel Riguidel, Telecom Paris-Tech, ENST, France; Aljosa Pasic and Fernando Kraus Sanchez, AToS; Jim Clarke and Keith Howker, Waterford IT;

cc to European Commission Unit F5, Trust and Security and Unit A2, International Relations.

BIC International Advisory Group (IAG) Terms of Reference

Background: During 2008 – 2010, there was an EU FP7 Coordination Action project entitled INCO-Trust[35] funded by the EU Commission's Unit F5, ICT Trust and Security research, which was engaged in bringing together EU researchers in the ICT Trust and Security communities with those in US, Australia, Japan, Korea and Canada. INCO-Trust concluded on 31st December 2011. Starting in January 2011, another coordination action project called BIC[36] (Building International Cooperation for Trustworthy ICT) was started again funded by the European Commission's Unit F5 ICT Trust and Security research – see http://cordis.europa.eu/fp7/ict/security/. The main goal of the **BIC** project is to build a long term strategy for International cooperation in ICT Trust and Security and to increase the coverage of countries (to include India, Brazil and South Africa) whilst maintaining and building the already established connections in the INCO-Trust countries. In order to maintain and strengthen the EU's international collaborations already established in INCO-Trust and bring them together with those being established in BIC, we are setting up an International Advisory Group (IAG) within BIC.

Structure and Implementation: In order to be effective, the IAG will be kept quite small with representation from each country based on:

- 1 (or more if deemed necessary by the country) member from the program management (funding body(ies)) associated with the funding mechanisms of Research and Technological Developments (RTD) related to ICT Trust and security, or whichever related title (or closest funding agency).
- 1 (see **note a.**) member of the RTD community, who has already engaged in international collaboration in ICT Trust and Security, and/or who can exhibit a genuine need and vision to participate in International collaboration activities. (**note a.** this number could be adjusted if the program management member suggests there should be additional RTD members required.)
- In addition, there will be "ex officio" members of the IAG e.g. BIC project members will take part in order to provide logistical and practical support including a secretariat function, together with a formal communication channel with the European Commission.

Membership: Membership of the IAG is on a personal basis. As a general rule, most of the involved funding bodies from each individual country already have programs in place looking at international cooperation, and in the past, they have covered their travel costs related to this type of networking with their counterparts in the EU. In addition, the meetings will be co-located with other relevant events/workshops in which the IAG members could attend to gain added benefit. The BIC project has allocated budget to cover administrative costs related to the venue, facility management and other organisational aspects and, in general, would not be in a position to cover the travel costs for the participants.

Effort and Time required: In addition to some audio conference style meetings when needed, it is envisaged there will be one annual forum consisting of a face to face meeting to coincide with other highly relevant events and workshops of interest.

Mission of IAG

- To facilitate collaborations between your national ICT Trust and Security constituencies and related ICT trust and security related constituencies from other countries; The IAG will be the forum bringing together the countries representatives from the earlier INCO-Trust participants and the BIC countries;
- To review the situation on International collaboration strategy in ICT trust and security on a regular basis providing advice on the priorities for international cooperation between the respective research communities, providing directions to the project and recommendations for improvement;
- Assist in the building of the working groups to enable BIC to structure relationships and linkages and facilitate contacts for theme based workshops or other networking events.

[35] **http://www.inco-trust.eu/**
[36] **http://www.bic-trust.eu/**