D3.1 - Interim recommendations report on future global research challenges in ICT trust and security

---

Grant Agreement number: 25258655

Project acronym: ***BIC***

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

Funding Scheme: ICT-2009.1.4 [Trustworthy ICT]

Project co-ordinator name, title and organisation:

James Clarke, Programme Manager, Waterford Institute of Technology

Tel: +353 71 9166628

Fax: + 353 51 341100

E-mail: jclarke@tssg.org

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

Table of Contents

1. Executive Summary 4
2. Introduction 5
3. Foreseeable bi-lateral co-operations between the EU and BIC countries 9
3.1 Europe 9
3.1.1 Background 9
3.1.2 Key research focus areas 10
3.2 Brazil 12
3.2.1 Background 12
3.2.2 The BR-EU coordinated call 13
3.2.3 Digital Identity – a major area identified between BR-EU. 13
3.2.4 Other common areas of interest within Trustworthy ICT between Europe and Brazil 14
3.2.5 BR-EU collaboration conclusions 15
3.3 South Africa 16
3.3.1 Background of Research funding agencies 16
3.3.2 Key research focus areas for collaboration 17
3.3.3 Conclusions 19
3.4 India 20
3.4.1 Background 20
3.4.2 Key research focus areas 21
3.4.3 Research Thrust areas in Cyber Security R&D department of DIT 22
3.4.4 Conclusions 25
3.5. Mapping analyses of the countries approaches to trustworthy ICT research 28
4.0 Strategy and recommendations for INCO in Trustworthy ICT research themes 38
4.1 Human oriented / citizen approaches to trust, privacy and security 38
4.1.1 ICT industry and the importance of societal and security challenges 38
4.1.2 Global approaches to technical and societal challenges 40
4.2 Network and Information security / cyber security 48
4.2.1 Evolution of threats and vulnerabilities 49
4.2.2 Threats and vulnerabilities in the years 2015 – 2020. 51
4.2.3 The fight against cybercrime. 53
4.2.4 Cooperation in cyber-defence against the asymmetric challenge. 54
4.2.5 Protective measures of defence and deterrence. 55
4.2.6 Cloud computing security companies. 57
4.3 Programme /funding focus/ identify community 58

4.4 The relationship between Europe and emerging countries 59

4.5 Regional Agreements 59

4. Conclusions 61

5.1 Future research challenges for international cooperation in trustworthy ICT identified across the BIC Working groups 61

5.1.1 WG1 *62*

5.1.2 WG2 *63*

5.1.3 WG3 *65*

5.2 Recommendations 65

5.2.1 Short-term recommendations (FP7 / 2013-14) *65*

5.2.2 Long-term recommendations (H2020 / 2015-20) *67*

6 References 71

1. Executive Summary

The purpose of the BIC coordination action project is fostering cooperation across the international funding agencies and researchers within the focus areas of ICT Trust and Security:

(a) in order to understand the activities and planning of the target countries; and

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

The building of international cooperation is a collaborative effort that only works if it reflects the views and priorities of the target countries as well as buy-in from technical experts of the EU along with the target countries. Hence, this component of community building is a key role of the Working Groups (WGs) of BIC as shown highlighted in figure 1. The areas and scope of the three working groups were agreed during the First BIC Annual forum in November 2011, including:

WG1 **Human oriented /citizen trust, privacy and security**, which will focus on topics related to a multi-disciplinary approach for international cooperation amongst all stakeholders;

WG2 **Network Information security / Cybersecurity,** which will focus on topics related to the need for international cooperation for enabling the protection of networks and systems;

WG3 **Programme/funding & focus/identify community**, which will focus on the requirements, processes, mechanisms and barriers to enable collaboration opportunities.

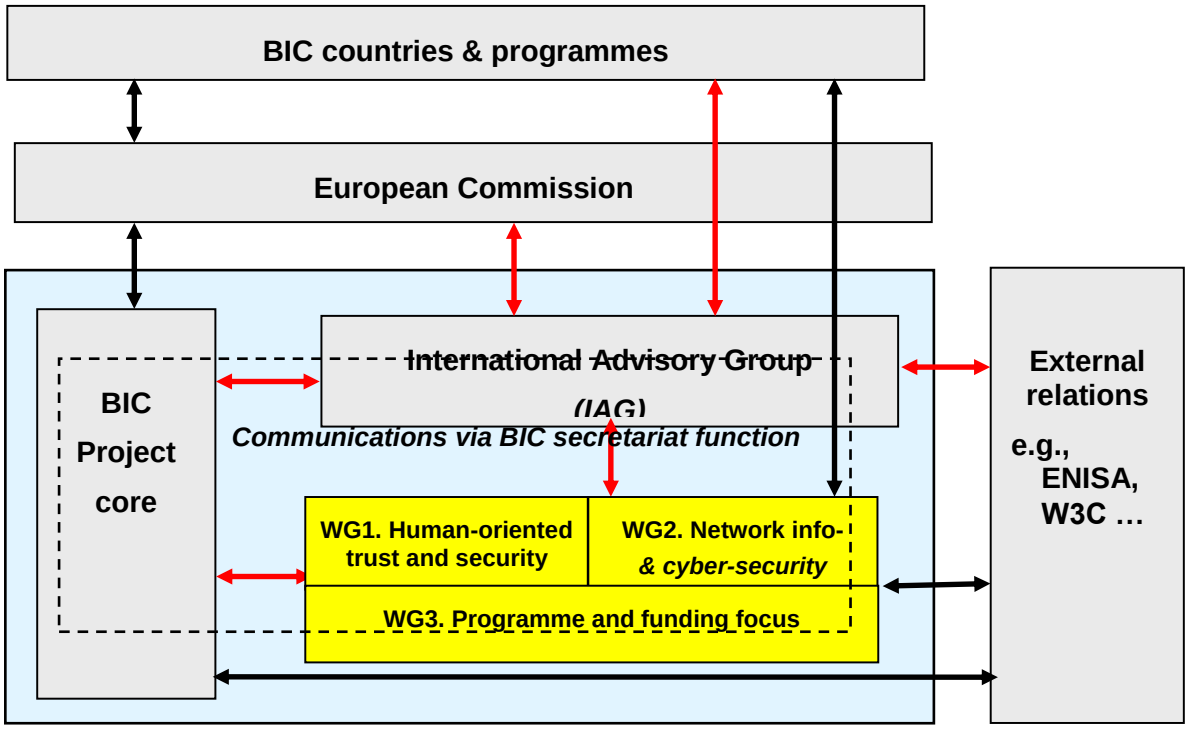

Figure 1. Overall structure of BIC project and external bodies

This deliverable is a report on interim recommendations on future global research challenges in ICT trust and security. It takes into account the bi-lateral workshops organised by the project in Year 1, the BIC planning session in July 2011, the annual forum in November 2011, and the BIC Working groups workshops held in June 2012. Special emphasis is given on the new entrants to the INCO community (via the BIC project) Brazil, India and South Africa. This report makes seventeen (17) short term recommendations for the remainder of FP7 (2013 – 2014) and twenty four (24) longer term recommendations for H2020 (2015 – 2020).

2. Introduction

This BIC interim recommendations report provides a first analysis of inputs received for the project's international platform building carried out in WP2/WP4. It also includes initial inputs from the Working Groups established by the project [1], its foreign visitations, workshops, and other activities and initiatives where BIC participated in and contributed to. This work has resulted in a set of interim recommendations for international cooperation in the fields of Trustworthy ICT research and technological development (RTD). These are broken down into two categories:

- Short term recommendations - for the remainder period of FP7 during 2013-14;
- Long Term recommendations - Horizon 2020 during 2015-20.

In line with the BIC goal to contribute towards the development of a mutually beneficial and long term strategy for international cooperation in Trustworthy ICT; and as discussed at our BIC Annual Forum held in November 2011 [2], three working groups are established. Their task is to develop a deeper understanding of important themes and topics that need to be tackled on a global basis in order to strengthen the EU's international collaborations within Trustworthy ICT, including the Trust, Security & Privacy areas.

These three working groups are the following:

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

The three BIC WGs are closely bound together in order to provide collaboration opportunities between them. The end goal is to contribute to a trusted and secure global digital communication and information handling – i.e. a secure and dependable international ICT infrastructure. This setup will be based on an evolving Internet, together with the many services that rely on it to deliver their benefits. The following summarises the coverage areas of the WGs (further details of these WGs are available in [1]).

WG1: Human oriented /citizen approaches to trust, privacy and security

This WG explores the human and societal dimensions of trust, privacy and security issues. These issues will affect the global social attitudes in general; however, the daily lives of the citizens of emerging economies is going to be greatly affected by the proliferation of information and communication technologies. This shift in the social behaviour of citizens requires reliable and fail-safe infrastructures as otherwise their abundant information including behavioural profiles will make them vulnerable to lifelong bullying.

The mapping of users evolves statistically. The number of digital users is constantly increasing in countries such as Brazil, India, China and Asia in general, so much so that we will witness a shift in terms of users in the next five years. The centre of gravity of users will be in the emerging countries (China, specifically).

Digital usages (from mobile phones and Internet devices) are spreading at an individual level, at companies and government institutions. The value of digital heritage has grown exponentially over the past decade. The proportion of sensitive heritage, in terms of confidentiality, has become a significant part to any physical or moral entity.

The techniques of cloud computing have focused on some applications. Outsourcing leads irreversibly to yield much of one's digital heritage to others. Such third parties are mostly located

abroad. Trust towards these third parties is generally not measured. The evolution of this trust over time is often unknown.

Social networks have exploded the private spheres. A large proportion of users are not afraid to display their privacy on these Web applications, they neither restrict in opinion posted, nor do they self-censor.

Blogs, microblogs are tools of growing use and importance, where freedom of expression is exercised in full in which users have been able to produce and work opinions into larger domains ever conceived possible before. There are numerous journalistic, photographic, musical and all kinds of other different blogs. People having opinions, expressing their views, attracting other people who care and agree/disagree with these opinions. Now, there are some negative aspects least of which is not only in the anonymity. There is also the problem with lies and, especially, half-truth and superficial treatment of complex questions. Often, these systems tend towards rapid propagation. Some statements – although wrong – cannot be easily proven wrong. Torrents of opinions, but sometimes also deluges of slander parade through blogs, spheres of subscribers and virtual friends of social networks, mostly using pseudonyms. Anonymity and pseudonymity are part of the combustion engine of this profusion of freedom in the expression where defamation and denigration can show off with impunity.

Widespread broadband Interconnection has led to instantaneous contact to organize combative events. Governments and authorities have become the target of attacks, either directly (Stuxnet attacks) or indirectly via these cyber-social systems (see the influence of digital tools in the Arab revolutions, see Wikileaks or Anonymous and Lulzec with their recent spectacular activities).

A new balance of power relationship is being established in each country where the asymmetric lever of digital tool takes a predominant dimension in order to communicate, to join the debate, to show opinions and to struggle. The digital behaviour has become a new dimension of the political and social space, whatever would be the political form of government (e.g. democracy, monarchy, dictatorship).

The conception of global digital ecosystem is changing the social landscape in an unprecedented pace. While the citizens need to be educated in such a way that reflects their local approaches, a global approach is equally needed to make the information highway safer for its commuters especially for its newcomers whose online behaviour will significantly affect the majority if not the entire community of the global surfers.

The initial recommendations would not have been possible without the inputs from the three BIC working groups:

WG2: Network Information security / Cybersecurity

This WG aims to investigate the security issues related to the global spread of computing and storage resources. Development of low cost and high speed networking technologies together with the fascinating business prospects of outsourcing is giving rise to more and more dispersion of ICT resources across the planet. The information stored in a location outside organisational/political control requires more checks and balances at technical as well as policy levels so as to ensure end-to-end security in a cyberspace.

The interconnection of networks has widened, extending into all developed, emerging and developing countries, and deepened with more robust and higher data rate transmission channels.

The physical and / or logical infrastructures move and adjust for several reasons, e.g. to save energy (moving data and storage centres in cooler regions for green ICT), in economically interesting countries (multinational and financial dimensions of Internet companies), or in countries where legislation is less constraining (digital paradise in terms of intellectual property). Furthermore, the localization of ICT activity (storage, computation) becomes technically difficult to determine and/or specify the location of resources in the network due to the emergence of massive distributed ICT.

The need for transparency of actions for actors on the networks has emerged in the recent years. This is especially the case of network neutrality, but this neutrality and transparency should extend, beyond networks, to service providers and content providers. These requirements are also moving the boundaries of the various international actors.

Distributed technologies (e. g. peer-to-peer techniques, mass-proxy systems) have dispersed the activities of communication, storage and computing, so that a user's hard to know the locations of its various operations.

The traditionally isolated users now feel power to act against the driving forces of the ecosystem, either network operators or service providers. These actors are oligarchies, pressure groups. Groups of these users are organized formally or informally to influence the future of the ecosystem.

Intellectual property (software and multimedia, music and video content) is mounted at the forefront of economic and legal issues to be resolved internationally, given the spraying of these contents over all continents and the impact of counterfeiting and illegal downloading. Content usage control is a thorny technical issue because there will never be 100% reliable security application with ad hoc heuristics depending on security by obscurity solutions. It is also a societal issue involving software patents, copyright, content distribution, management of digital content, DRM).

Assuring overall security of a cyberspace is not a trivial task. Any shortcoming in the security linchpin may result in global meltdown of the consumer trust in these infrastructures. Globalisation of ICT resources is itself the weakest link of the security chain. Moreover, the extent of liabilities in the advent of breaches poses too many risks to be taken by some businesses specially SMEs. This situation is exacerbated by the lack of demarcation of responsibilities in a virtual world. It is therefore necessary to tailor security solutions to address the peculiar needs of the cyberspace.

WG3: Programme /funding focus/ identify community

This WG investigates the holistic approach for a comprehensive security program. Its objective is to take a broader overview of the security requirements not limited to the social issues and technical solutions. Availability of enormous computing and storage resources are the prime mover of innovation. However, the same resources are increasingly becoming invaluable assets for the people with nefarious intentions.

Cyber surveillance of the ecosystem by governments but also by public or private actors has become a major concern. Humanistic values, free speech, privacy of personal data and digital behaviour, privacy and human dignity must be respected across networks. Whistleblower punishment and free speech support are contradictory. Neither of these issues is of technical nature and has to do with policy. It has become easier to disseminate information largely, it has not become easier to be noticed; that has actually become more difficult in the increased background noise.

The commodification of personal data (making money from personal data collection) has become a scourge by the collection, the capitalization of profiles database and the sale of directories with names, addresses or identity attributes. The business model of sites and Web applications development based on the number of subscribers or users, has facilitated capture of data without consent, black market and fraudulent use of directories for inappropriate usages. This phenomenon is technology-driven. Mass-crawling and mass-evaluation are possible because of the world-scale availability and search of personal data. That has not existed before the internet, web, search engines and OSN.

Statistical heuristics for profiling people, even using anonymous data has become problematic. Previously sufficiently well anonymised data as data of the Census Bureau and the like, can now be partly de-anonymised using the available public data on the internet, be it from the search engines and OSN or from dedicated wholesale companies. Databases, to exploit the personal data, are made in the greatest secrecy, without the consent of individuals. The large availability of data samples on the Internet gives a statistical base for a broad testing of individuals in publicly available polls, both commercial and governmental. The data mining tools and the test data are publicly available. There

is often no need to do anything in secrecy; it suffices to download e.g. publicly available (fully anonymised) US governmental statistics and to make an analysis using personal data. Depending on the art of data processing, about 3% of records can be identified by doing so.

Faced with this stunning deployment of polymorphic converted architectures and new services, methodologies and tools of security have not changed, while threats have expanded in two key dimensions: the fragility of the personal assets of individuals and the possible destabilization of large institutions due to various movements caused by the widespread interconnection and end-to-end high data rate: cyberhaktivism (Anonymous, Wikileaks) and cyber-terrorism (attacks reaching states).

Disruptive security tools have tended to stagnate over the past ten years. This decrease in clean-slate research has produced gaps that are difficult to fill in 2012. Digital security tools have not been able to organize with additional tools on trust between a system and its user. The instruments of trust have not made any progress. Trust models are not yet finalized. However, compared to 1995, security has made some significant progress; technologically and in terms of real deployment. Today, cryptography is in almost every piece of software. Lightweight security exists. New models involving context have been proposed and work on IDS, honeypots have progressed. OS security has made tremendous progress, with some vendors leading the way. Security indicators now get published. ISO 2700x introduced security management. All larger companies have security officers and spend resources on security. Secure computation has recently been theoretically solved. Private communications have been invented (onion routing). There is no decrease in research; the funding of security has increased. The acceptance of importance of IT security has also improved. Public sensitivity to IT security has improved.

However, for the most part, this work has been undertaken in isolation in countries and it is now the time for the international research communities to pool their resources in order to ensure that their security research emphasises the anticipation and identification of new threats and vulnerabilities and developing new methods and tools to address and counter the attacks.

There are number of challenges in formulating a universal security program. Different institutions and cultures have different rather conflicting perception of security threats. The scope of security solutions and their enforcement methodologies are also the bone of contention among various communities. It is, therefore, necessary to initiate some dialogue at the international level to work out the common security goals and to develop some interoperable mechanisms to reach these goals.

Report Structure

This deliverable is organised in the following sections:

Section 3 is entitled ***Foreseeable bi-lateral co-operations between the EU and BIC countries*** and summarises the intensive analysis of BIC countries. This analysis was carried out on a bi-lateral basis in the first year of the project through workshops, visitations, the annual forum and continued contacts with the working group members.

Section 4, entitled ***Strategy and recommendations for INCO in Trustworthy ICT research themes*** consolidates recommendations for the promotion of international cooperation on research into the initial themes as developed by the working groups of BIC: human oriented approaches to trust and security, network and information security and global alignment of the communities to attain our longer term strategy for international cooperation amongst countries. These recommendations take into account the new aspects of trustworthy ICT, especially those who have a broad and international impact, either because it requires joint reflection and cooperation in research to solve issues in the medium to longer term, or because the consequences of arising phenomena have an instantaneous impact, direct or indirect, beyond the borders of the continents.

Section 5, **Conclusions** summaries the deliverable. In general, security requires a combined effort at the highest level to promote interoperability between methodologies and tools to enable internationally better dialogue and standardization frameworks in order to benchmark, compare and exchange information so as to enhance the development of digital and services infrastructures.

3. Foreseeable bi-lateral co-operations between the EU and BIC countries

This section examines the findings from the BIC Countries Brazil, South Africa and India. As this report can be considered a stand-alone document, this section also includes a summary of the EU approaches to trust and security research for the readers from outside Europe.

3.1 Europe

3.1.1 Background

Europe recognises that it needs an effective digital global strategy and R & D instruments adapted to the multi-factorial crisis being experienced. This is still possible while most European countries have yet engineers and talented researchers in this area. The various members of Europe are often in heartbreaking competition with each other, while the real intellectual and economic competition exists internationally. Europeans are not just consumers and the vision of the European digital ecosystem should not focus on one economic or architectural construction of the bi-lateral consumer-producer or client-server. Digital science must be developed in all its societal dimensions, by extending its infrastructure, and then by its support for any human activity, focusing on industrial activities, only capable of spreading faster growth and jobs.

The computer sometimes requires international cooperation for the definition of standards, especially in hardware or in software interfaces. However, in applications, consultation is increasingly unnecessary: we must be bold, imaginative in the design, and speed and courage for the dissemination and exploitation in the global market.

An area in which the European Union has placed primary emphasis is on the development of “Trustworthy ICTs” that respect citizens' rights and protect their privacy and personal data. It believes that security, trust and privacy issues need to be coherently addressed from a technological, economic, legal and social perspective, in an effort to ensure innovation and economic growth in a society providing freedom and security for its citizens.

In operational terms, the European Commission's Directorate General (DG) Information Society and Media (DG-INFSO), through its "Trust and Security" unit F5, through which the BIC project is funded, has been entrusted with supporting and coordinating research across the continent and through international cooperation. Research priorities in this domain are strongly related to the development of the Future Internet and target:

- trustworthy network and service infrastructures,
- user-centric identity and privacy management
- technologies for secure software development, trusted computing, cryptology and advanced biometrics.

Furthermore, DG-INFSO provides interoperability and standardisation support, when appropriate, to strengthen the societal impact of the technology results. It stresses particular emphasis on the horizontal aspects of trust and security in ICT, by highlighting multidisciplinary research and the relevance of aspects like usability, societal acceptance and economic and legal viability of the research results.

Through DG-INFSO Unit F5, the European Union has a legacy of supporting rich collaborative research in Trust and Security areas. European experience shows that this is best done by leveraging the diversity of its constituents and also by engaging in active international cooperation with promising non-European countries, in order to build a comprehensive approach to identifying issues and problems, pool technology and resources and craft solutions that address major existing and potential Trust and Security issues across the vast domains of ICT infrastructure, platforms, devices, services and solutions in democratic and pluralistic societies.

As of 1st July 2012, DG-INFSO is becoming DG CONNECT (Communications Networks, Content and Technology) and the trust and security unit leaves the former INFSO Directorate F "Emerging Technologies and Infrastructures" and becomes a part of CONNECT Directorate H "Sustainable and Secure Society". Directorate's H's main goals are to address selected ICT challenges for a sustainable, healthy and secure society, and to develop a full-cycle roadmap to get the output into the EU economy, through innovation tools such as pilot-lines, pre-commercial procurement, and standards. Directorate H is the leader for Horizon 2020/Societal Challenges.

The Trust & Security (H.4) unit priorities are the following:

- Elaborate a European strategy on Internet security and remove Cyber security related obstacles to the proper functioning of the Internal Market.
- We will manage implementation of the e-privacy Directive and follow-up of all issues related to the protection of privacy on-line.
- Manage the various financial programmes (FP7, CIP, H2020) supporting the Internet and ICT security.
- Promote a better coordinated and coherent approach on cyber incident management worldwide.

To find out more information about the transition to DG CONNECT, please follow

http://ec.europa.eu/dgs/information_society/connect_en.htm

3.1.2 Key research focus areas

Objective ICT-2011.1.4 Trustworthy ICT has the following target outcomes:

Heterogeneous networked, service and computing environments

Trustworthy (meta) architectures and protocols for scalability and interoperability, taking account of heterogeneity of domains, partitions, compartments, capabilities and environments in ecosystems and underlying infrastructures; architectural standards, including meta-level specifications, for conformity, emergency and security policy management.

A trustworthy polymorphic future internet with strong physical security in balance with privacy; federated, seamless, transparent and user-friendly security of the edge networks in smart ecosystems, ensuring interoperability throughout the heterogeneous landscape of access networks.

Virtualisation and other techniques to provide protection, assurance and integrity in complex, high-demand critical services; and security in the presence of scarce resources, and in legal domains with different priorities. Trustworthy global computing with contextual security and secure smart services in the cloud.

Metrics and tools for quantitative security assessment and predictive security in complex environments and for composition and evaluation of large scale systems.

Enabling technologies, such as declarative languages, biometry, technology for certification and accreditation or cryptography for Trustworthy ICT.

Trust, e-Identity and Privacy management infrastructures

Development of trust architectures, protocols and models for trust assurance, including measures and rating models, and services and devices to enable trust assessment (e.g. by claims on identity, reputation, recommendation, frequentation, voting), to delegate trust and partial trust; and for trust instrumentation and high-level tools at the end-user stage (cognitive and learning instrumentation for trust, profiling services and communities).

Protocols for privacy infrastructures enabling multi-identity and tools to check privacy assurance and enable un-observability and un-linkability through search engines or social networks. Advancement of privacy at the hardware level.

Interoperable or federated management of identity claims integrating flexible user-centric privacy, accountability, non-repudiation, traceability as well as the right to oblivion at the design level. Technologies and standardisation for use of multiple authentication devices, applicable to a diversity of services and ecosystems, and providing auditing, reporting and access control.

Data policy, governance and socio-economic ecosystems

Management and governance frameworks for consistent expression and interpretation of security and trust policies in data governance and means for implementation, including in the ubiquitous scale-less Web or Cloud. Technology supported socio-economics frameworks for risk analysis, liability assignment, insurance and certification to improve security and trust economics in the EU single market.

Multi-polar governance and security policies between a large number of participating and competitive stakeholders, including mutual recognition security frameworks for competing operators; transparent security for re-balancing the unfair, unequal face-to-face relationship of the end-user in front of the network; tools for trust measurement, based on cost-benefit analysis.

Networking and Coordination activities

Support for networking, road-mapping, coordination and awareness raising of research and its results in Trustworthy ICT.

Priority will be given to (i) stimulating and organising the interplay between technology development and legal, social and economic research through multi-disciplinary research communities; (ii) promoting standards, certification and best practices; (iii) coordination of national RTD activities.

Expected impact:

Improved European industrial competitiveness in markets of trustworthy ICT, by: facilitating economic conditions for wide take-up of results; offering clear business opportunities and consumer choice in usable innovative technologies; and increased awareness of the potential and relevance of trustworthy ICT.

Adequate support to users to make informed decisions on the trustworthiness of ICT.

Increased confidence in the use of ICT by EU citizens and businesses. Increased usability and societal acceptance of ICT through understanding of legal and societal consequences.

Demonstrable improvement (i) of the trustworthiness of increasingly large scale heterogeneous networks and systems and (ii) in protecting against and handling of network threats and attacks and the reduction of security incidents.

Significant contribution to the development of trustworthy European infrastructures and frameworks for network services; improved interoperability and support to standardisation. Demonstrable usability and societal acceptance of proposed handling of information and privacy.

Improved coordination and integration of research activities in Europe or internationally.

The new work programme for WP2013 will be available shortly.

3.2 Brazil

3.2.1 Background

The following list contains an overview of Brazil´s Research and Development (R&D) priorities according to the Ministry of Science and Technology (MCT) - 2007-2010 plan, which includes the following areas of research:

- ICT
- Nanotechnology
- Biotechnology
- Technological Development of Enterprises
- Nuclear Policy
- Space Programme
- Management of Ecosystems
- Energy and Mineral Resources
- Climate Change
- Meteorology, Climatology & Hydrology
- Biodiesel
- Hydrogen and Fuel Cells
- Biodiversity
- Antarctica

ICT priorities for the 2010 European and Brazil (EU-BR) coordinated call have been stated as:

- Future Internet - Experimental Facilities
- Future Internet - Security
- e-infrastructures
- Networked Systems and Control
- Microelectronics/Microsystems

The area of Future Internet - Security was justified according to the 2010-2014 National Plan for Broadband Access in Brazil, where the government intends to reduce the actual regional and social disparities to information broadband access: South-East 23,81%, South 21,33%, Center-West 20,45%, North 13,45%, and North-East 4%. For this the government has investments in the order of R$ 49 billions (EUR 18 billions) to fixed single access type (urban and rural) to guarantee in 2014 around 30 millions of broadband access.

Considering the Community Fixed Access the goals are:

- 100% broadband access for government institutions
- 100% Federal Administration
- 100% Public schools
- 100% health centers (more than 177.000)
- 100% public libraries (more than 10.000)
- 100% public security institutions (more than 14.000)
- Create 100.000 federal telecenters.

Considering the mobile access the goal for 2014 is 60 millions of broadband mobile access in the country.

Many challenges are introduced according to the necessary scenario transformation for Future Internet – Trust and Security priority area in Brazil. For digital inclusion, citizens must trust the environments. This cannot be based solely on technology, a trusted system should incorporate technological, social and legal guarantees. Solutions that are globally relevant will have the greatest impact and hence the longer benefit, and consequently international cooperation is mandatory.

Within Brazil, there are a number of funding agencies for ICT related research in Brazil:

CNPq (National Research Council) and FINEP (financiadora de estudos e projetos) have public calls for funding. These are national foundations linked to the Ministry of Science and Technology. More information at http://www.cnpq.br/english/cnpq/index.htm and http://www.finep.gov.br/english/FINEP_folder_ingles.pdf.

CTIC is the Research and Development Centre for ICT of the Ministry of Science and Technology. They are an alternative to CNPQ but with focus in ICT. Currently, they have several funding lines, one in DigitalTV, another in Cloud Computing, another in Smart Cities and another in Network Virtualization. Website can be found at http://www.ctic.rnp.br/

FUNTEL, which is a fund for technological development of Telecommunications. FUNTEL is linked to the Ministry of Communications of Brazil. http://www.funtel.com.br

State Research Foundations - Each State has its own foundation with its own budget and they have freedom to establish their own calls, but it is not only specific to ICT.

3.2.2 The BR-EU coordinated call

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

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

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

Although this call is now completed, further information on it can be found here:

The Coordinated Call between European Union and Brazil

http://cordis.europa.eu/fp7/dc/index.cfm?fuseaction=UserSite.CooperationDetailsCallPage&call_id=377

The call was also released in Brazil under a call for proposals issued by CNPq

http://www.cnpq.br/editais/ct/2010/066.htm (in Portuguese).

Within WP2013, there is expected another ICT-2013.10.2 EU-Brazil Research and Development Cooperation. The topics for consideration include:

a) Cloud computing for Science
b) Sustainable technologies for a Smarter Society
c) Smart Services and applications for a Smarter Society
d) Hybrid broadcast-broadband TV applications and services.

3.2.3 Digital Identity – a major area identified between BR-EU.

A survey of the activities undertaken by RNP (Rede Nacional de Ensino e Pesquisa) in the area of identity management was presented at the BIC workshop as an area of potential cooperation

between EU and Brazil. RNP is a non-profit, non-government organization that acts as Brazil's NREN (National Research and Education Network). Besides being responsible for Internet access of more than 300 organizations, RNP maintains a portfolio of services for the academic community.

The model that is adopted for the development of new services is to have part of RNP's research and development team maintain a working group program. This program, which was formally launched in 2002, issues an open call once a year. The selected groups have one year to develop a prototype of the proposed service. After this, some of the resulting prototypes are selected for a second phase, in which the group develops a pilot of the service. If the pilot is successful, it becomes an experimental service, and finally, after one more year, goes into production. Over the 10 years of the program, several services have successfully reached production. Examples are video streaming and distribution, voice over IP, distance-learning tools, and services related to authentication and authorization.

In the area of authentication and authorization, two independent groups led efforts related, respectively, to public key infrastructures and to federated authentication and authorization. The first of these efforts resulted in ICPEDU, a PKI for the academic community. Prof. Ricardo Custodio, from UFSC (Universidade Federal de Santa Catarina), led the PKI efforts, and currently the root CA is maintained by his institution. The efforts of the second group led to the creation of CAFe, a federation for access to web-based services in which authentication is provided by the users' home organizations, known as their Identity Providers. Service Providers receive information about authentication and other attributes necessary for access control from these Identity Providers, creating a trust network.

RNP has now created a Technical Committee for Identity Management (CT- GId), with members from RNP itself and from the academic community, with the goal of overseeing the evolution and integration of identity-related services. One of the first activities of this Committee was to recommend the implementation of a pilot eduroam federation, for access to wifi networks. This is being demonstrated in the end of May 2011 at RNP's annual workshop (WRNP). Other foreseen activities include proposals for the integration of the Brazilian PKI and Federation with their international counterparts and the fostering of the use of these technologies in different scenarios.

The presentation and subsequent discussions concluded with a more in depth explanation of how to become involved in Working Groups. A pointer was made to the annual Brazilian Symposium on Security, which may be an interesting opportunity to interact with the Brazilian research community: http://www.ppgee.unb.br/sbseg2011/sbseg2011.html .

3.2.4 Other common areas of interest within Trustworthy ICT between Europe and Brazil

- Cloud Computing & Cloud Storage is increasingly "the" international conduit for data and knowledge sharing along with the corresponding international impact implications if its trustworthiness gets compromised across the internationally diverse physical, human and functional elements.
- While there are a multitude of technical activities of mutual interest, the issues of data governance and liability are key themes that need to be addressed from both a policy and technology viewpoint.
- As the Internet of Things also relates to the cloud model, the nature of legally and globally consistent identifiers of both people and "things" required international harmonization.
- Infrastructures Integrity is a dedicated international association issue for infrastructures spanning the telecommunication SLA's behind the cloud and the Future Internet, or for the financial and services sector (data centres, service and support centres etc). Similar to the cloud issues, the policy issues of governance and liability are critical.
- International Data exchange capabilities and dataset sharing: The interconnections across computing systems and data on an international scale require coordination as countermeasures across globally penetrative security attacks. A repository of globally

accessibly attacks and countermeasures repository would form a high international interest activity.

- Security Compliance Management and Information Security Assurance is a key international policy element that needs to be developed to link the above technical issues, and very much needs to be detailed from a multi-national and multi-cultural viewpoint. A necessary element to develop is the economics of security from an international compliance, governance and provenance aspect.
- Future Internet data and information provenance (trusted source) especially during times of disaster and large events is a topic that was highlighted at the session, for mutual cooperation between Brazil and the EU. Recent examples (e.g. Japan earthquake and subsequent tsunami) were discussed at length in which the reliability of information becomes extremely questionable for long periods due to the vicious cycle of feeding untrustworthy or incorrect information between conduits via the 'new media'. For a more trustworthy Future Internet, the user must be able to categorically trust the source and integrity of the data and information they are receiving. There are complementary skills in Europe and Brazil on these research topics and they can be leveraged well together on this topic.

3.2.5 BRAZIL-EU collaboration conclusions

In recent years, there have been a number of productive joint activities held already between the EU and Brazil in looking at collaborations between the countries:

- In September 2009, there were two international workshops held in Brazil examining EU-Brazil cooperation on new architectures for the FI.
- A coordinated call was already held in EU FP7 call 7 between the EU and Brazil including one topic on Future Internet - Security.

One of the goals of the BIC project is to follow the considerable Brazil – EU joint efforts already done and to increase productive joint activities and collaboration between the EU and Brazil research communities.

A number of potential technical areas and initiatives for further mutual collaboration were identified between Brazilian and EU researchers in Trustworthy ICT. These are summarised here.

- Digital Identity and global compatibility (interoperability). A potential for this collaboration could be interoperable trustworthy "identity spaces", which refer to identity domains that range from social networking sites to a country level where the government is acting as an identity provider (for unique electronic ID documents). While we can assume that government issued e-IDs (with qualified certificate) are going to be accepted by a number of service providers and individuals using the services (but not all), many service combinations and aggregations will pose issues of interoperability due to varying levels of assurance and non-existence of internationally conformant metrics. Closely related is the notion of identity and privacy assurance. There is a need to jointly agree on the description of components and security requirements as well as offered identity management or privacy capabilities that would ease the security assurance of composed systems from an international data access perspective and EU compliant privacy laws.
- Security metrics and assurance: both European and Brazilian participants shared a joint vision that there is a need to have internationally recognised criteria for security metrics and assurance and that further collaboration on user acceptance and confidence in solutions such as service compositions or cloud computing, should be fostered.
- Security and privacy: in collection of data from heterogeneous sources, design, composition, discovery and delivery of context-aware secure services are pinpointed as objectives for many participants. Technologies such as the Near Field Communication (NFC), for example, ease the collection of contextual data and link a service such as payment to an actual physical location. Other proximity sensor technologies such as Bluetooth, Wi-Fi or barcodes

pose similar problems and the setting of associated privacy rules seems not to be sufficient since the preferences can be very dynamic while users trust varies from location to location.

- Privacy by design principles: closely related to a specific service business model should help the user in the management of this location information. The integration of sensor networks with social networks is another example of applications that can sense the context, provide new services, but also extend the notion of "identifiable" data. Context can be also observed on micro-blogging services such as Twitter.
- Future Internet: environments that combine sensors (Internet of Things), social networks (Internet of People) and service provision (Internet of Services) involve event-related security information that must be understandable independently of language, age, physical condition, social status, or education of the recipient. This is an important aspect where Brazil has a great deal of experience and track record in the past, such as in the design of their installed Automated Teller Machines (ATM) machines in the 1970's in which a rigorous design process involving customers was followed in the user interface design resulting in extremely user friendly interfaces. In the Future Internet (FI), context-aware services and devices with localization systems will be offering attractive new functionality. People who travel and need access in mobile international environment, such as, for example, tourists or business people, will use not only contents but likely other services such as on-line collaboration, context-aware social networking or trusted local services such as emergency related or mobile payment services. The challenge for a "roaming" user will be to discover and use only 100% trusted and secure services where origin and data provenance can be verified. There is work ongoing in Brazil on this topic and the participants exhibited a willingness to work together with Europe on this.
- Universality of trust and privacy: Concerns about trust and privacy are universal. Citizens on the move are especially sensitive and vulnerable targets given that different platforms, service providers, organizations, business processes, policies and technologies may be involved within international service-chain provision. Therefore, user-centric security, trust and privacy configuration sets are needed. As a user typically uses the same device in multiple contexts, assistance or even automation of adaptation of configuration to a specific context is needed. It is important, therefore, to provide adaptable and context-aware privacy protection mechanisms and tools for automatic customization and personalization of security services.
- Standardisation: Privacy is one of the research issues that is highly subjective and contextual and there is a need for the agreement and publications of standards for WS-Agreement, and similar web service protocols, while the Semantic Web technologies for Secure Web Services may be yet further investigated while the community reaches consensus on the appropriate approach. Europe is ahead in the research on this topic.
- International cooperation in Cyber-security: The need of a comprehensive research towards international Intelligence, Surveillance, and Reconnaissance (ISR) in the cyberspace domain was highlighted by some participants, as the interdependent network of IT infrastructures is considered to be one global domain within the information environment, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. Furthermore, the ability to conduct comprehensive intelligence collection on any threatening of our cyberspace activity followed by near-simultaneous processing, exploiting and disseminating of the information depends on international collaboration, data and knowledge exchange and sharing between all countries.

3.3 South Africa

The following topics were found to be of interest to both countries.

3.3.1 Background of Research funding agencies

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

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

3.3.2 Key research focus areas for collaboration

Trust Management for techno-socio business ecosystems in the context of emerging economies

A techno-socio business ecosystem in the context of Emerging Economies is defined as a collaborative on-line and real time trading environment where large enterprises (LEs) such as suppliers and financial institutions transact with Very Small Enterprises (VSEs) such as small retail stores. In the majority of cases these VSEs are operating from remote and rural areas and have a lack of ICT infrastructure. VSEs use mobile phones to interact with the techno-socio business ecosystem.

Many sociological and cultural differences prevent the trusted interaction amongst VSEs; between LEs and VSEs; and in general between rural communities and mainstream commerce.

As there is a large level of variation in the acceptance of social and other controls that govern trust between the different types of participants in these business ecosystems, this poses a major challenge. In order to support collaboration and interaction, the development of an “indigenous trust model” for such communities is required. An “indigenous trust model” in the context of this proposal is a model that reflects the unique requirements of emerging economies such as the concept of focusing on people's allegiances (Ubuntu). A trust model needs to be defined over the premises that rural participants, such as VSEs, may be more likely to trust an application (technological system) if they experience a sense of normality because their familiar social controls are present in the systems.

As the concept of community and community leaders is of special importance to rural people in the African context, it is suggested that this concept be incorporated in trust models for deploying technology (applications) in these communities. Consider for example the following:

The formation of groups and clusters of people in local communities. These groups are formed not only on similar types of participants but also on similar needs. A good example in South Africa is the concept of “Stokvel” whereby a syndicate of people does pooling of financial resources.

Community leaders as moderators of trust. This is useful where a participant needs to transact with a stranger who is part of a community as the community leader may provide a trusted introduction.

The envisaged trust model for mobile applications in emerging economies will be based on agent technology that collects and stores feedback about participants, build reputation of participants and share reputation information with others.

International Cyber security research – added value of the African perspective

A question that was raised a number of occasions with the South Africa researchers was: "Could Africa become the home of the world's largest botnet or an unbridled cyber security pandemic?" This is at least a possible scenario given the fast pace of increased broadband (and largely wireless) internet penetration in Africa, where there is currently very low broadband penetration in many areas, high levels of computer illiteracy, sometimes ineffective legislation, and where anti-virus software may be un-affordable or too technically sophisticated for the low-cost devices that are still used. This heterogeneous continent harbours a large socio-techno-digital divide that needs to be accounted for in first-world security solutions since this world is connected to the developed world through the opportunities and challenges of the internet.

International, collaborative research can address these challenges by looking at a variety of approaches that require innovative implementation, including:

ISPs taking a bigger role / responsibility with the provision of security services so that much less depends critically on the end user (i.e. creating "thin clients" vs the "thick client" where the ISP only provides the pipeline).

Bottom-up, community oriented approaches to Critical Information Infrastructure Protection.

Sector based cyber security alliances (universities, industries, banks) that share information / best practice.

Opening up international data-exchange architectures for cyber security.

Models and platforms for national and regional cybersecurity coordination (citizens, industry, security sector, government, regional governments).

Financial Infrastructure protection

The financial sector is particularly challenged by their need for providing secure eBanking in the face of a barrage of sophisticated, creative, efficient and persistent phishing attacks. The banks are providing competitive eBanking services for computers and mobile devices but regard reducing and fighting crime as a shared and non-competitive responsibility. This can benefit hugely from public-private-partnerships including the current close cooperation with the Police as well as local and international research collaboration on issues such as:

Mathematical analysis of normal vs abnormal patterns in banking behaviour.

Packaging abnormal behaviour (suspicious behaviour, attack vectors).

Anonymising the shared data and information to effectively address concerns about reputation loss, paramount client privacy and anti-competition laws.

Establishing a Financial Sector Computer Security Incident Response Team (CSIRT) that meets international standards for reducing risk and responding to incidents. South Africa has already had collaboration with ENISA, EU CSIRTs, USA and others.

Leveraging technical developments in the mobile and cellular networks to provide increased trust as well as usability of eBanking solutions.

South African Law enforcement approaches to deal with cybercrime

The SA Law Enforcement agencies have to deal with a variety of cyber crimes with significant criminal intent including increasingly sophisticated social engineering, customised Trojans and commercial spyware, computers and information for sale, "ransomware" (the next level "scareware"), attacks on mobile devices and even signs of attacks on automobile computer systems. There are strong signs of this being organised cyber crime with the criminals operating directly or by proxy from just about anywhere in the world.

This is already addressed through closely intertwined and good relations between law enforcement and technology providers e.g. ISPs on a national basis, adopting a mutually supportive strategy. These relationships assist with the capturing and justly punishing of the cybercriminals which is necessary in order to impact criminal business models. However, there is still a large gap between sentencing for physical crime vs cyber-crime.

International, collaborative research should give direction to the serious challenges with the prevention/combating, investigation and prosecution of cross-border cyber-crime. This requires adaption of everything from policy to legislation to technology strategy.

Better coordination of the country's cross border cyber crime detection and prevention is not currently prioritised. How can this effectively be elevated to the highest authority? What is the national "business case" for increased attention, coordination and funding?

EU approach towards trust and security in the Future Internet

South Africa does not currently have an active debate regarding the Future Internet, as is the case in Europe and elsewhere. This crucial debate is shaping the creation of the next generation of the Internet with an increase of Internet based services. The physical and virtual worlds are converging. There is a revolution in data networks such as LTE. Open delivery platforms are becoming the norm.

While the developing world including South Africa is catching up and mobilising the current Internet, and wrestling with the trust, security and privacy issues that it brings, it also needs to be ready for the Future Internet. This is as true for governments as it is for industry, and it is clear that any Future Internet will require significant public-private-partnerships.

The EU can assist through collaborative international research enabled by the ongoing Future Internet activities and these were discussed during the workshop. Examples include the FI-PPP and the Future Internet Assembly in which a number of the participants BIC project are key members.

3.3.3 Conclusions

The collaboration between the South Africa researchers has enabled the process of identifying topics of cooperation that would be of mutual benefit to the EU and South Africa in the research fields of ICT Trust and Security.

In addition, a number of follow up activities were identified that would benefit and increase collaboration between the EU and South Africa research teams:

- 4th EuroAfrica-ICT Cooperation Forum on ICT Research, 14-15 November 2011, Cape Town, South Africa: The BIC project including the participation of the DG INFSO Head of Unit organised a special Session on Building International Collaboration on Trustworthy ICT, including presentations from the BIC project team members. With the broader African / European attendance, this session was used to convey the outcomes of the BIC Workshop at the ISSA2011 conference and added further value and clarity to joint EU/Africa research priorities in Trustworthy ICT.

- South African Trust and Security Research Database: Establishing such a database will be taken up with the ISSA conference organisers as a way of supporting international

collaboration and access to knowledge and research skills. This will also be cross - correlated with the work being done in BIC in building the trust and security research community.

- The University of Johannesburg is driving the establishment of a South African Academic Cybersecurity Alliance that will, among other things, arrange a yearly Cybersecurity Awareness Day that could link with international awareness efforts of BIC.

3.4 India

3.4.1 Background

The fast emergence of the information and communication technology (ICT) sector in India economy has placed this country on the digital world scene in the past fifteen years. The Indian ICT sector has grown at a remarkable rate and the flow of information has brought knowledge to the information society creating new opportunities for all sectors (government, education, transport, health, finance, commerce). New applications and services that use ICT infrastructure capabilities are emerging at an ever increasing pace. The industry focused first on exports, which were growing year on year when compared to the domestic ICT market; but the domestic growth in ICT overtook the ICT exports, over the last decade. The domestic demand in ICT has shifted from hardware towards an ICT solutions approach, with a growing emphasis on services. India has a very large pool of skilled, low cost, English-speaking manpower, compared with other countries. India is also characterized by rapid growth in the telecom sector with a subscriber base increasing at an average of 8 million per month. The telecom sector in India is promising in terms of number of telephone subscribers reaching the 500 million and new internet connections moving to 40 million. On the one side, there are a lot of opportunities offered by the web world to break barriers. On the other side, the digital divide could take at least a decade to achieve an all-inclusive growth. The intense volume of information and the simplicity of its transfer pose challenges that require intervention by the government and call for strengthening of the Indian IT regulatory framework to address cross border issues. Increased focus is being placed on capability growth in bandwidth (mobile and wireless networking technology), data communication speeds, and a trained skilful workforce. With government support for R&D, India is emerging as a major player in the ICT world.

Within India, ICT is crucial to daily operations of organizations and government. Personal lives involve computing in areas ranging from communications with family and friends to online banking and other household and financial management activities. Enterprises are reliant on ICT to be able to operate, to support business processes, including R&D. Critical infrastructures, such as those related with telecommunications system, air traffic control, energy, healthcare, banking and finance, defence, law enforcement, transportation, water systems, and government, are indispensable for the modern society and depend on ICT-based systems and networks. The ICT infrastructure has become an integral part of the ‘critical infrastructures’ in India as it has around the world. The failure of the current ICT technologies or best practices to meet an expected service level might have a significant impact on society. Cyber-attacks on Indian information networks or key economic functions can have serious consequences such as disrupting critical operations, eroding public trust in information systems, causing loss of revenue and intellectual property, or loss of life. Countering such attacks requires the development of robust capabilities to reduce vulnerabilities and deter those with the capabilities and intent to harm critical infrastructures. Understanding the intersection between critical infrastructure systems and the ICT systems increasingly used to control them is a common theme for research needs. An emerging issue is that infrastructures, until now autonomous, are becoming intertwined into network-of-networks. It is this interconnection where the ICT play a pivotal role.

There is a very active community of researchers engaged in trust and security research within India. Through their initial contacts and in subsequent contacts made during the project, the BIC project participants have been able to work closely with the researchers to collectively scope their particular research areas of interest. Although the research funding in India is mainly academic and research institution focussed, we have found that industry is well complemented by the Universities, such as the Indian Institutes of Technologies (IIT’s) and the Indian Institutes of Information

Technology (IIIT's). Therefore, our focus for interactions has been with all the stakeholders, and this has resulted in a better understanding of the research communities' needs for increasing engagement with the EU.

3.4.2 Key research focus areas

During the BIC organised workshop in December 2011 during eIndia 2011 to scope trust and security themes, the key focus areas were discussed with the India participants. The most predominant discussion point was the risks associated with current and anticipated vulnerabilities of, threats to, and attacks against the ICT infrastructure. In summary, the main Indian areas of concern with regard to trust and security are:

The increasing complexity of IT systems and networks, which will present mounting security challenges for both the providers and consumers.

The evolving nature of the telecommunications infrastructure, as the traditional phone system and IT networks converge into a more unified architecture.

The expanding mobile and wireless connectivity to individual devices, computers and networks, which increases their exposure to attack. In hybrid or all-wireless network environments, the traditional defensive approach of securing the perimeter is not effective because it is increasingly difficult to determine the physical and logical boundaries of networks.

The increasing interconnectivity and accessibility of (and consequently, risk to) computer-based systems that are critical to the country's economy, including supply chain management systems, financial sector networks, and distributed control systems for factories and utilities.

The breadth and increasingly global nature of the IT supply chain, which will increase opportunities for subversion from attackers within and outside the country.

These concerns have prompted the Indian ICT policy and research planners to focus research priorities on a range of topics that would mitigate existing and emerging threats and provide network and information security in order to make the IT networks 'Trustworthy' for the large variety of users, from government running the affairs of the country to gamers enjoying an online session on their home computers.

The policy, articulated by the DIT Cyber Security R&D Group[1] when they met with BIC in December 2011, which is the closest to the Trust and security unit in the European Commission lays emphasis across the spectrum - Basic research, Technology demonstration and Proof-of concept and R&D test bed projects. It stems from the consideration that indigenous R&D is an essential component of national Information strategy in order to:

- mitigate export restrictions on sophisticated products by advanced countries;
- build confidence that an imported IT security product itself does not turn out to be a veiled security threat;
- create knowledge and expertise to face new and emerging security challenges;
- produce cost-effective, tailor-made indigenous security solutions and even compete for export;
- market in information security products and services.

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

3.4.3 Research Thrust areas in Cyber Security R&D department of DIT

The areas of near to medium term public-funded Information Security research in India under the aegis of the Cyber Security R&D department within the Department of Information Technology (DIT) are :

Cryptography and Cryptanalysis

- Algorithms and applications, software and hardware realisation, FPGA, VLSI, DSP, smart cards for security, protocol analysers;
- Authentication and authorisation techniques, role based access rights, Biometric identification/authentication systems, Trust models and technologies that do not rely on a previously determined trusted third party, in dynamic environment

Network and Systems Security

- Virtual Private Network Security solutions;
- Security of key internet protocols (IPv4 to IPv6), Domain Name System (DNS) and Border Gateway Protocol (BGP), routers, servers;
- Security of wireless devices, protocols and networks;
- OS Security and trusted OS;
- Automatic generation of test suites, safe programming languages;
- XML security.

Security Architectures

- Survivable architectures and intrusion tolerant systems that allow for degradation of certain capabilities, while ensuring that critical functionality remains available;
- Autonomic systems that can sense and reason about their internal components and state and recovery oriented computing;
- Self-evolving systems/ Self-strengthening systems that can monitor themselves and adapt to change;
- - Secure and survivable storage systems.

Vulnerability and Assurance

Vulnerability Detection and Analysis

- Source / Object code scanning tools, Device (hardware, firmware, communication media, storage media) scanning tools, Host and network based scanners, system configuration checkers;
- Tools and techniques for modelling interdependencies and vulnerabilities in systems;
- Risk analysis tools.

Assurance Technologies

- Tools for efficient product evaluation and system level evaluation;
- Assurance tools for software security;
- Network Audit Tools.

Monitoring, Surveillance and Forensics

Intrusion Detection

- Virus scanning, malicious code detection;
- Firewalls, Intrusion Detection Systems (network and host based), distributed and intelligent;
- proactive Intrusion Detection Systems;

- Intrusion detection for high speed networks.

Content and Traffic Analysis

- Cracking code/passwords /logs;
- Content filtering tools for Indian and other languages;
- Intelligence gathering tools;
- Intelligent traffic analysis;
- steganography and steganalysis.

Computer Forensics

- Computer forensic tools for speech and imaging;
- Automated trace-back tools, Network forensics;
- Automated Recovery, damage assessment and asset restoration tools.

In addition to the key thrust areas of trust and security of most interest to India as published in their work programme, a number of key observations were made during the discussion sessions of the BIC workshops.

These include the following:

- The Indian approach to trust and security in ICT is functional, rather than conceptual. The main concentration is on the 'plumbing' or 'nuts and bolts' rather than a focus on the concepts behind the design of the systems.
- Indian research in 'Trust and Security' areas focuses predominantly on Indian competitiveness, technological edge, import substitution, functional areas, networks, devices and architectures, rather than having a 'service to end user' perspective in its articulation.
- Trust, privacy and security in India are not sufficiently appreciated from the perspective of citizens' rights, benefits for business and society's entitlements, although there is a strong community led by the Data Security Council of India advocating strong privacy and data protection as a lever for economic development of India through global integration of practices and standards conforming to various legal regimes and promoting India as a global 'secure' place to conduct business. The published mission of the Data Security Council of India is "To create trustworthiness of Indian companies as global sourcing service providers, and to assure clients worldwide that India is a secure destination for outsourcing where privacy and protection of customer data are enshrined in the global best practices followed by the industry." [14]
- There is a serious concern with the security, integrity and reliability of hardware, especially when highly reliant on imports in India.
- Unique Identification (UID) project: How to guarantee protection of the citizen's rights, security, privacy in the context of the mammoth Unique Identification (UID) project, which is currently in the roll out phase.
- The increasing complexity of IT systems and networks and expanding mobile and wireless connectivity present mounting security challenges, which substantially increases their exposure to attack.
- The level of the Indian cryptography research is very high (e.g. the famous "Primes is in P" result showing that there is an elegant deterministic polynomial time algorithm for primality testing of integers secure OS standards for smart cards at IIT Kanpur, etc.); idem for theoretical and practical aspects of cryptography, number theory, computational complexity.
- The level of the Indian mathematics research is well recognized in applied mathematics: data mining and machine learning, formal approaches to security.
- CERT (Cyber Emergency Response Team) to be a premier reference in Asia Pacific Region (New Zealand, Vietnam, Australia, Korea…).
- Data and Intellectual Property (IP) vision needs to be improved to become a secure country for data and IP. IP risks due to employee turnover.

- Cyber forensics for tracking attackers and enforcement purposes, protection against the social network of hacker groups, and establishing their Modus Operandi; Promoting awareness in cyber-security among students through ethical hacking contest.
- Multilinguism issues in trust and security: language-independent information dissemination using NFC. Multilingual systems are a serious challenge in India.
- Cybercrime (virus in email, trojan in webpage, fraud in ecommerce transactions, e-robbery in e-banking transaction, identity theft in credit card payment).
- Terrorism on physical telecom infrastructures (fixed or wireless telecommunication network operations) and cyber-terrorism with unlimited resources and motivation or cyber warfare with rogue nations.
- • Development of trust models for cloud computing: client authenticated policy enforcement mechanism for the cloud; building Trusted Platform; Privacy preserving processing on the cloud. However, there was a strong opinion from the researchers that broadband coverage issues within India should be addressed in a more serious way before the cloud could become a major topic of coverage in trust and security.
- Security of Mobile telecoms; and building trust for Mobile transactions.
- Cryptographic protocols between Payment System Provider, Deposits, Payment and Authorization) for micro-payment is highly suited for India.
- E-governance, information sharing, surveillance and analysis: to foster collaboration between federal, state, and local agencies as well as the private sector.

List of ongoing projects

The following is a list of ongoing projects funded by the DIT Cyber Security R&D department:

1. Project title: Development of test bed for Information Security skill development using Virtual Training Environment (VTE)
   Project coordinator: Alok tripathi, sr. design engineer, DOEACC Society, Gorakhpur, gkp.alok@gmail.com
   Project objectives: To design and simulate various scenario based problems and solutions using virtual training environment systems with associated lab manuals for Incident handling, Intrusion analysis, Perimeter security, Hardening of systems, Network Security testing, Cyber Forensics.
2. Project title: Development of Person Authentication System based on Speaker Verification in Uncontrolled Environment
   Project Coordinator: Dr. S. R. Mahadeva Prasanna, Associate Professor, Indian Institute of Technology, Guwahati-781039, Assam, prasanna@iitg.ernet.in
   Project objectives: 1) Development of speaker verification database in multilingual, multi-sensor and uncontrolled environment; 2) Research and development of a speaker verification system for speech data collected from uncontrolled environment; 3) Development of person authentication system using speech and one of the non-biometric features like PIN targeted to phone banking.
3. Project title: Cyber Forensics & Digital Analysis Centre in short to be known as "Cyber Centre"
   Project coordinator: Shri B. Ramani, CDAC, Thiru and Shri Tomin.J. Thachankary, IPS, IGP, SCRB, Kerala Police Thiruvananthapuram, gkp.alok@gmail.com
   Project Objectives: 1) To establish a State of Art Cyber Forensics and Digital Analysis Centre in Kerala for the benefit of Law Enforcement Agencies and other Stake holders; 2) To develop Human "Resources to handle matters related to Cyber" Forensics from among various stake holders; 3) To educate even the students in basics of Cyber Forensics as a preventive measure against cyber crimes; 4) To conduct real case analysis and give expert opinion in crime cases, civil disputes to facilitate investigation and to assist Courts; 5) To reduce the burden on the Cyber Forensics Resources Centre of C-DAC Tvpm in order to give more time to the Scientists of C-DAC, Tvpm for Research and Development.

4. Project title: CYBER & HI-TECH CRIME INVESTIGATION and training
   Project coordinator: Director, CBI Academy Ghaziabad, CBI Academy, Ghaziabad, Gorakhpur- 273010, gkp.alok@gmail.com
   Project Objectives: To impart training to cyber crime investigators, forensic examiners and Trainers and potential Trainers of the Police Training Institutions in the country in the fields of - (i) Cyber Crime Investigation and (ii) Cyber Forensics.

3.4.4 Conclusions

Following the mapping exercises and analysis (see Annex 1), the following topics have been identified as a first list of potential topics by the EU and India researchers for mutually beneficial cooperation in the area of trust and security. They are grouped in five general themes.

Theme 1: Digital ecosystem trustworthiness

This theme is oriented towards securing the current as well as the Future Internet (Infrastructure, applications, services, data, etc.), the crisis management systems at all granularities (time & space) for enterprises and institutions; asymmetric challenge: cyber-haktivism, frauds, cyber-terrorism and security models: interoperability, subsidiarity, multidisciplinary: security embedded within existing context, ambience and culture.

CERT: A cooperation to enhance the security ICT realm through proactive action and competent collaboration is required for the current exploitation of the ICT infrastructures (internet, mobile telecoms). International cooperation must be enhanced in this area in order to create awareness about DDOS, BOTS, phishing, etc. Figure 2 contains details of the Indian Computer Emergency Response Team: statistics from 2010.

Protection against malware: when there is a heavy reliance on imported systems as in India: approaches to influence the manufacturing process and to guarantee protection at source.

Figure 2: Indian Computer Emergency Response Team: statistics from 2010.

Theme 2: Trust & Privacy

This second theme is oriented towards human oriented security, privacy (Identity & anonymity frameworks, accountability, e-reputation) and trust measurement and management, dignity (e-reputation, rumours, non-solicited information (pub + spams).

Language-independent Security: security usability is a major challenge for any culture and any country: return of experience from outside could be beneficial for both continents. India and Europe are continents where several languages and several scripts. Usability for alarms, alerts, warnings is an important factor for improving the understanding of the mechanisms and awareness of security. Cooperation could benefit to both continents.

Trust, Security and Privacy in mobile environments: mobile connectivity that accommodates the heterogeneity and failure-proneness of both devices and network to gel with issues such as broadband and sparse coverage in India. Also, the need for usable security in the mobile environment e.g. the simple elements of data integrity and security that lets people “trust” the devices to do banking and other activities given that the mobile platform is the sole/primary platform for many users in India.

Identity management (e.g. India’s UID, EU’s privacy protecting ID systems): biometrics – Europe and India could work together on low cost, less power intensive equipment providing the required accuracy. Authentication, built upon the strong work in India and EU, could mutually improve potential future solutions.

Strong societal push in both EU and India: Putting citizens in control of their data and how can technologies provide this control to citizens? Forging strong link between social scientists and technologists. How to deal with conflicts between the "right to info", "access to personal data", "updating the data" and right-to anonymity (be forgotten).

Balance between strong security tools and efficiency and effectiveness - Security with flexibility; building cost effective, tailor made, indigenous security products that compete for export market. These tools will also be helpful in ensuring the compliance of data security – such as encrypted storage of personal data. Data controllers can effectively manage the bulk of data if proper tools for security compliance are available within their reach.

Theme 3: Global Framework and international alignment

The third theme of cooperation is concerned by interoperability of the subsidiarity security models, policy, governance and data exchange for cyber-security and the socio-economic area.

Convergence of physical and cyber worlds: To ensure the security of society either in the physical world or the cyber-world requires coming together of all stakeholders with a collaborative effort. We need to share experiences on building secure knowledge society.

Appropriate regulations: Policy makers must find appropriate regulations in order to coordinate efforts from different stakeholders to try to develop a roadmap of cyber-security practices that will be sharpened in the future in order to ensure a leading role of Europe and India together in the global digital economy.

International Data Exchange for Cybersecurity: Secure data exchange and sharing for analysis and CERTs working well together. Sharing of information with the stakeholders of the digital ecosystems is becoming a milestone in combating cybercrimes. An increasing number of regulators are therefore developing new rules for enforcing data sharing (e.g. data breach notification by ENISA). Enforcement of such obligations in a cyberspace is an uphill task as stakeholders especially businesses have strong opposition for these measures. Such obligation of sharing data is often seen as a double-edged sword that may result in loosing the customer confidence on the businesses; or

make them liable to penalties if some business critical security breach information is not shared with the stakeholders.

Attackers and Hackers: There is a need to work together on addressing the international data exchange and sharing of information and intelligence on cyber-attacks for a free flow of the information in a secure and reliable manner. To collectively fight against cyber-threats an organized response is requested to understand the emerging threats and identify solutions and create a roadmap of actionable activity schemes.

Intellectual Property: Cooperation to create a platform for promoting sharing of knowledge about information security and foster the community.

Risk management approaches to trust and security: Looking at the economics of security and privacy. Trade-offs between risk and security: what does it cost to society?

Theme 4: Engineering and Scientific domains

The fourth theme concentrates on the constant effort in models (cryptography, security models), methods and tools (, information systems, networks, hardware, software) to improve the science methods and the engineering process for the discipline.

Cryptography - Cooperation with the centre of Mathematics and Cryptography (the Indian Statistical Institute (Kolkata), ITT (Kanpur, Chennai, Kharagpur) for stream ciphers, hash functions, provable security, elliptic curve pairing theory, secure multi-party computations, steganalysis, side channel cryptanalysis; E-passport.

Cyber Forensics – RTD in software tools for use in forensic investigations in today's ICT environments (cloud computing, mobile etc.). This is a topic of importance in India where they would like to work with the EU researchers that was raised at the BIC workshop.

Security of payment - Social engineering attacks and malicious traffic attacks are priorities, due to the increase usage and growing commercial importance of user-centric online services.

Security enforcement tools – A number of authentication and authorisation tools find their roots in the classical system security where assets were more tangible and limited in number. They have adapted to the emerging scalable and virtual systems. However, increasing security requirements of global cyber infrastructure require an extensive overhauling of these methodologies and tools to workout their effectiveness in the contemporary distributed systems.

Theme 5: International Cooperation on Cyber-security

The fifth theme is international cooperation specifically on the topic of cyber-security as it is a global issue, requesting a global approach to alleviate the increasing ICT-related risks. To be successful, international cooperation to promote cyber-security must be built on sound national organizational structures. National strategies to promote cyber-security have to take into account the different stakeholders and existing initiatives. Countries should adopt a multi-stakeholder approach, based on dialogue, partnership and broad participation in order to benefit all stakeholders.

The growth of a digital ubiquitous, ecosystem has pushed innovation of enormous value for the global economy and society. The meta-system construction with software, hardware, and digital data has created a critical infrastructure upon which the smooth functioning of essential sectors depends. While providing societal benefits, this exciting opportunity has also produced a major and growing complex of risks for all countries around the world. Interdependencies of global economies expose them to the vulnerabilities of each and every member state. The overall security of the cyberspace cannot be ensured if one or more segments of this realm remain volatile and therefore exploitable by some malicious elements.

There is a need to improve data, network and computer security around the globe as governments, businesses, consumers and citizens are faced with an increasing variety of cyber-threats and critical infrastructure requires protection from cyber-attacks. Starting by setting best practices for the exchange of cyber-security information between countries, operational institutions (CERT) and governmental agencies need to involve the R&D sector to be supported following the extremely fast evolution of vulnerabilities.

International research programmes with joint efforts between nations could be launched to further research into cyber threats and vulnerabilities. An international cooperation could bring together business, government, and academic experts to frame the key issues for cooperation on cyber-security. These efforts could lay foundations for a framework for international cooperation in cyber-security.

Maintaining trustworthy digital infrastructure requires addressing many problems as systems can be compromised by a weakness in any aspect of a component or network. A trustworthy infrastructure should be secured by design, but it should also be able to detect, prevent, and survive attacks. Thus, cyber-security research must encompass a large range of ICT disciplines: technological (data, software, network, cryptology, etc.) and societal (economy, ethics, sociology, criminology, etc.).

Already links have been established by BIC with the International cooperation directorate at the DIT and a meeting of the EU – India High Level Working Group was held in Q1 2012, whose intention is to further pursue actions on further mechanisms for joint India – EU cooperation on a number of topics, including ICT Trust and Security. BIC provided input to this meeting through their contacts in the other EU – India CSAs and directly through the Commission. In addition, BIC made a presentation to the DIT before this meeting so they were very aware of the ICT Trust and Security topics of interest between the countries.

3.5. Mapping analyses of the countries approaches to trustworthy ICT research

In this section, the approaches of Brazil, India, South Africa and the EU towards ICT trust and security are analysed and mapped together in order to establish a number of potential areas for cooperation with EU that would take into account the varying different perspectives. The following table contains the mapping of the countries perspectives.

The overall focus of ICT trust and security research in the seventh Framework Programme is on developing knowledge and technologies for building an open, secure and trustworthy information society in Europe where citizens and organizations can fully reap the benefits from the new technologies. Central to the research is enabling users to manage and protect their digital assets, identities and personal data when they interact in the digital world.

Closely interrelated thematic areas are promoted as target outcomes inside the of topic “trustworthy ICT”, including:

1. Heterogeneous networked service and computing environments, including Architectures and protocols; Future Internet; Virtualisation and other techniques for protection, assurance; Metrics and tools for quantitative security; and Enabling technologies (languages, biometry, crypto, ..).

2. Trust, eID and Privacy management Infrastructures, including Trust assurance; Privacy infrastructures; and Management of ID claims (usability, privacy, control).

3. Data policy, governance and socio-economic ecosystems, including Management and governance frameworks for trust and security policies; Technology supported socio-economics frameworks; Multi-polar security governance; and Tools for trust measurement.

4. Networking and Coordination Activities, regarding Stimulating and organising interplay technology-law-society-economy; Promoting standards, certification, best practices; and Coordination national RTD activities.

Brazil	India	South Africa	EU
General Approach for ICT security and trust			
The Brazilian approach to trust and security in ICT is to secure the underlying infrastructure being deployed especially mobile infrastructure. The digital divide across the regions notably in the northern Amazonian region is of great importance. The geographical as well as cultural diversity of the country induce infrastructural vulnerabilities that need to be stemmed out. A necessary element to be developed by the country is the economics of security from an international compliance, governance and provenance aspect.	The Indian approach to trust and security in ICT is functional, rather than conceptual. The main concentration is on the 'plumbing' or 'nuts and bolts' rather than a focus on the concepts behind the design of the systems. Cultural diversity of India has resulted in the multilingual systems. These systems are a serious challenge in India. The country needs to develop language-independent information dissemination using NFC.	The South African approach to trust and security in ICT is to reinforce the education of the various segments of society so as to produce qualified indigenous manpower and to raise awareness of the general public.	The EU approach is to examine (or make attempts) to examine the in-depth concepts and horizontal aspects for trust, privacy and security e.g. empowering the users to gain control over trust, security and privacy issues. Emphasising the horizontal aspects of trust and security in ICT by highlighting multi-disciplinary research and the relevance of aspects like usability, societal acceptance and economic and legal viability of the research results. Europe also boasts the diversity of languages and scripts. However, security issues of multilingualism are underestimated in Europe.

Brazil	India	South Africa	EU
Theoretical Frameworks: Assurance, Identity, Cryptography, Security Metrics and formal Models			
Security metrics and assurance is a need to have internationally recognised criteria for security metrics and assurance and that further collaboration on user acceptance and confidence in solutions such as service compositions or cloud computing, should be fostered.	The Indian universities and research centres produce high quality mathematicians who excel in modelling techniques. Therefore, the level of the Indian cryptography research is very high (e.g. the famous “Primes is in P” result showing that there is an elegant deterministic polynomial time algorithm for primality testing of integers secure OS standards for smart cards at IIT Kanpur); theoretical and practical aspects of cryptography, number theory, computational complexity. The level of the Indian mathematics research is recognized in applied mathematics: data mining and machine learning, formal approaches to security. It has been found that cryptographic protocols between Payment System Provider, Deposits, Payment and Authorization) for micro-payment is highly suited for India.	The South African government intends to make some headway in the area of theoretical and fundamental research activities in pure and applied sciences including ICT domains.	Increasing the leadership of the European cryptography skill that is recognized at the international level. There is a significant on-going work in formal methods for trust and security engineering.

Brazil	India	South Africa	EU
Security of Applications and Data: data exchange, data governance and IPR			
Future Internet data and information provenance (trusted source) especially during disasters and large events is a topic for mutual cooperation between Brazil and the EU. There are complementary skills in Europe and Brazil on these research topics that can be leveraged well together on this topic. International Data exchange capabilities and dataset sharing: The interconnections across computing systems and data on an international scale require coordination as countermeasures across globally penetrative security attacks. A repository of globally accessibly attacks and countermeasures would form an activity of high international interest. Cloud Computing & Cloud Storage is a global paradigm for data and knowledge sharing along with the corresponding international impact implications if its trustworthiness gets compromised across the internationally diverse physical, human and functional elements.	Data and Intellectual Property vision needs to be improved to become a secure country for data and IP. IP risks due to employee turnover. Tracking attackers, and the social network of hacker groups, and establishing their Modus Operandi. Promoting awareness in cyber-security among students through ethical hacking contest. E-governance, information sharing, surveillance and analysis: to foster collaboration among federal, state, and local agencies as well as the private sector.	Financial Infrastructure protection: The financial sector is particularly challenged by their need for providing secure eBanking in the face of a barrage of sophisticated, creative, efficient and persistent phishing attacks. The banks are providing competitive eBanking services for computers and mobile devices. However, they regard reducing and fighting crime as a shared and non-competitive responsibility. Financial infrastructure protection can benefit hugely from public-private-partnerships including the current close cooperation with the Police as well as local and international research collaboration on issues such as: - Establishing a Financial Sector Computer Security Incident Response Team (CSIRT) that meets international standards for reducing risk and responding to incidents. South Africa has already established collaborations with ENISA, EU CSIRTs, USA and others.	Europe has strict legislation on the rights and obligations with digital data. Enabling technologies for security and trustworthiness of ICT that guarantee rights, address security, trust and protect the privacy and personal data of the users and enable participative governance. Intellectual Property: developing standards for the industry and creating awareness among stakeholders about security and privacy issues. The issues of data governance and liability are key themes that need to be addressed from both policy and technology viewpoint. For a more trustworthy Future Internet, the user must be able to categorically trust the source and integrity of the data and the information they are receiving Addressing the international data exchange and sharing of information and intelligence on cyber-attacks for a free flow of the information in a

Brazil	India	South Africa	EU
Security of Applications and Data: data exchange, data governance and IPR			
Infrastructures Integrity is a dedicated international association issue for infrastructures spanning the telecommunication SLA's behind the cloud and the Future Internet, or for the financial and services sector (data centres, service and support centres etc.). Similar to the cloud issues, the policy issues of governance and liability are critical.		Financial infrastructure protection can benefit hugely from public-private-partnerships including the current close cooperation with the Police as well as local and international research collaboration on issues such as: - Mathematical analysis of normal vs. abnormal patterns in banking behaviour. - Packaging abnormal behaviour (suspicious behaviour, attack vectors). - Anonymising the shared data and information to effectively address concerns about reputation loss, paramount client privacy and anti-competition laws. - Leveraging technical developments in the mobile and cellular networks to provide increased trust as well as usability of eBanking solutions.	secure and reliable manner.

Brazil	India	South Africa	EU
Trust and Privacy			
Trust, Security Compliance Management and Information Security Assurance are key international policy elements that need to be developed. They need to be detailed from a multi-national and multi-cultural viewpoint. Privacy: in collection of data from heterogeneous sources, design, composition, discovery and delivery of context-aware secure services. Privacy by design principles: closely related to a specific service business model should help the users in the management of this location information. Universality of trust and privacy: Concerns about trust and privacy are universal. Citizens on the move are especially sensitive and vulnerable targets given that different platforms, service providers, organizations, business processes, policies and technologies may be involved within international service-chain provision. Therefore, user-	Trust in India is not sufficiently appreciated from the perspective of citizens' rights, benefits for business and society's entitlements (although there is a strong community advocating the need for this!). There is a serious concern with the security, integrity and reliability of hardware. How to guarantee protection of the citizen's rights, security, privacy in the context of the mammoth Unique Identification (UID) project, which is currently in the roll out phase. Indian research in Trust focuses predominantly on Indian competitivity, technological edge, import substitution, functional areas, networks, devices and architectures, rather than having a 'service to end user' perspective in its articulation. Development of Trust models for Cloud Computing: client authenticated policy enforcement mechanism for the cloud; building Trusted Platform; Privacy preserving processing on the Cloud.	Trust Management for techno-socio business ecosystems in the context of Emerging Economies. A techno-socio business ecosystem in the context of Emerging Economies is defined as a collaborative on-line and real time trading environment where large enterprises (LEs) such as suppliers and financial institutions transact with Very Small Enterprises (VSEs) such as small retail stores	Trust is an important concern to improve security and enable interoperability of heterogeneous cloud platforms. Current research projects are proposing trust models to solve this major issue. Significant work is still required. Privacy is one of the research issues that are highly subjective and contextual and there is a need for the agreement and publications of standards for WS-Agreement, and similar web service protocols. While the Semantic Web technologies for Secure Web Services may be yet further investigated while the community reaches consensus on the appropriate approach. Europe is ahead in the research on this topic. Concept of 'Privacy by Design' embedding privacy proactively into technology, thereby ensuring full privacy and data protection and the 'Identity Management' Supporting and coordinating research across the continent and through international cooperation by prioritising the development of the

Brazil	India	South Africa	EU
Trust and Privacy			
centric security, trust and privacy configuration sets are needed. As a user typically uses the same device in multiple contexts, assistance or even automation of adaptation of configuration to a specific context is needed. It is therefore important to provide adaptable and context-aware privacy protection mechanisms and tools for automatic customization and personalization of security services.			'Future Internet' Balancing between the right to anonymity (privacy) and the societal imperative of making personal data available.

Brazil	India	South Africa	EU
Resilience of Infrastructures and Physical Infrastructure Protection			
Future Internet: environments that combine sensors (Internet of Things), social networks (Internet of People) and service provision (Internet of Services) involve event-related security information that must be understandable independent of language, age, physical condition, social status, or education of the recipient. This is an important aspect where Brazil has a great deal of experience and track record in the past, such as in the design of their installed Automated Teller Machines (ATM) machines in the 1970's in which a rigorous design process involving customers was followed in the user interface design resulting in extremely user friendly interfaces. In the Future Internet (FI), context-aware services and devices with localization systems will be offering attractive new functionality. People who travel and need access in mobile international environment, such as tourists or businessmen, will use not only contents but likely other services such as on-line collaborations, context-aware social	Terrorism on physical telecom infrastructures (fix or wireless telecommunication network operations) and cyber-terrorism with unlimited resources and motivation or cyber warfare with rogue nations. Security of Mobile telecom; building trust for Mobile transactions. The increasing complexity of IT systems and networks and expanding wireless connectivity present mounting security challenges that substantially increase their exposure to attack.	Cybercrime (virus in email, Trojan in webpage, fraud in ecommerce transaction, e-robbery in e-banking transaction, identity theft in credit card payment). Lack of ICT infrastructure and use of mobile phones to interact with the techno-socio business ecosystem. Security of Mobile telecom; building trust for Mobile transactions. Development of contextual Trust models depending upon education, culture ("indigenous trust model"). South African Law Enforcement approaches to deal with cybercrime: The SA Law Enforcement agencies have to deal with a variety of cybercrimes with significant criminal intent including increasingly sophisticated social engineering, customised Trojans and commercial spyware, computers and information for sale, "ransomware" (the next level "scareware"), attacks on mobile devices and even signs of	Physical infrastructures: European industry may be underestimating the threat to Internet security posed by physical attacks to telecommunications infrastructure. Potential vulnerabilities of the critical infrastructures underpinning the Future Internet and Cloud Computing environments need to be identified by Europe in order to minimize the impact and the frequency of threats. Ensuring the CERT in Europe is tracking attacks and sends out periodic advisories and generates statistics and trends in cyber-attacks. Malicious attacks: European researchers are mostly concerned by the data misuse followed by network-oriented issues such as malicious traffic attacks or data integrity on the network itself. Industry experts put breaches of trust within companies and misuse of personal information – for example through Facebook or e-banking – as their number one internet security concern. Vulnerabilities in emerging Cloud environments due to reduced ownership of resources and data is also a concern. International

Brazil	India	South Africa	EU
Resilience of Infrastructures and Physical Infrastructure Protection			
networking or trusted local services such as emergency related or mobile payment services. The challenge for a "roaming" user will be to discover and use only 100% trusted and secure services where origin and data provenance can be verified. The Internet of Things related to the cloud model, the nature of legally and globally consistent identifiers of both people and "things" requires international harmonization.		attacks on automobile computer systems. There are strong signs of this being organised cybercrime with the criminals operating directly or by proxy from anywhere in the world. This is already addressed through closely intertwined and good relationships between law enforcement agencies and technology providers e.g. ISPs adopting a mutually supportive strategy at national level. These relationships assist with the capturing and prosecuting the cybercriminals that is necessary in order to impact criminal business models. However, there is still a large gap between sentencing for physical crime vs cybercrime. The increasing complexity of IT systems and networks and expanding wireless connectivity present mounting security challenges that substantially increase their exposure to attack.	cooperation in Cyber-security: The need of a comprehensive research towards international Intelligence, Surveillance, and Reconnaissance (ISR) in the cyberspace domain was highlighted by some participants, as the interdependent network of IT infrastructures is considered to be one global domain within the information environment, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. Furthermore, the ability to conduct comprehensive intelligence collection on any threatening of our cyberspace activity followed by near-simultaneous processing, exploiting and disseminating of the information depends on international collaboration, data and knowledge exchange and sharing between all countries. The fight against fraud and cybercrime is implemented in each country with a relatively good efficiency. The behaviour of the attackers is reduced to playing hide and seek with the police on the internet. This niche is more and more narrow and difficult. The

Brazil	India	South Africa	EU
Resilience of Infrastructures and Physical Infrastructure Protection			
			attacker status is different in some emerging countries (Asia, Africa, South America) where the legislation is not yet enforced or the means to fight against cyber-criminality are not yet deployed.

4.0 Strategy and recommendations for INCO in Trustworthy ICT research themes

This chapter develops contributions to a long-term strategy for international cooperation based upon the initial themes as developed by the bi-lateral workshops held in year 1, the annual forum and the working groups of BIC:

WG1. Human oriented /citizen approaches to trust, privacy and security, which will focus on topics related to a multi-disciplinary approach for international cooperation amongst all stakeholders;

WG2. Network Information security / Cybersecurity, which will focus on topics related to the need for international cooperation for enabling the protection of networks and systems;

WG3. Programme /funding focus/ identify community, which will focus on the requirements, processes, mechanisms and barriers to enable collaboration opportunities.

Wherever appropriate in each section throughout the section text, BIC proposes a number of short term (for remainder of FP7 during 2013/2014) and long term recommendations (for H2020 on the period 2015 – 2020) towards areas for future international research in trust and security.

4.1 Human oriented / citizen approaches to trust, privacy and security

4.1.1 ICT industry and the importance of societal and security challenges

Home phone, tablets or computers have become familiar objects. The Web, search engines, e-commerce, social networks are daily tools, pledges of opportunities, contacts, knowledge and innovation. While such tools have become indispensable in everyday life, digital era has essentially become the backbone of all high-tech industry (space, aviation, telecommunications, finance, health, automotive), industry production (energy, food) and is now at the core of organizations, services and administration.

The digital ecosystem is not limited to internet, phone and television. The geo-navigation services with the future Galileo system, smart grids for future energy savings, information logistics, microelectronics, credit cards and contactless cards, high powerful computers and the whole software industry are an integral part of this dynamic and structuring ecosystem for human activity.

The digital ecosystem is in constant metamorphosis, steeped in an intellectual and social environment that deeply transforms this medium, which is reacting and influencing in turn the uncertain trajectory of digital systems, both in their technology and their practices. The decisions and actions to intervene in the control of this highly dynamic ecosystem can only be strategic and long term. A conscious policy to develop economic growth or improving the security of critical infrastructure must anticipate the future of our digital society and not just legislate on the consequences of adverse effects in technology and usage changes.

The main developments that need to be addressed in research include:

What will be tomorrow's digital ecosystem, what is the future of the basic infrastructure (Internet, 3G/4G, Galileo) irrigating countries? What part should one invest in networks, high performance computers, services, search engines? What reliability for the digital urbanisation, still under construction? What is the impact on society and the environment?

What are the economic and social changes? What will be the new value chain in the digital world? What are the various sustainable socio-economic models in the digital space between digital stakeholders and end users? What are the business models between the various players in the ecosystem (between access, service and content providers)? How to manage the diversity of public and private intangible assets? What will be the share between citizens, administrations and companies?

What will be the usage transformations (managing diverse digital identities and their attributes in the private sphere, the circulation of files and property notions)? How to define and manage the side of identity (or pseudonym and therefore accountability) and its opposite side of anonymity in cyberspace?

What protections can we use against constant, increasingly violent, massive, scattered and anonymous attacks? How to beat the international filing by calculation that plagues the entire e-commerce and social networks with the black market of directories with names, addresses and digital behaviour? What impact on education (what relationship between digital information and all other school subjects)? What global governance and national subsidiarity for these fragmented and intersecting sub-ecosystems?

Short-term recommendations (FP7 / 2013-14)

STR1. Awareness raising programmes for general public should be developed to increase awareness and skills in secure use of the digital world. Human users are the weakest link in the security chain. It has often emerged that some security breaches or online frauds could have avoided if users were properly trained. The overall objective of these programmes should not be to make people frightened of the digital world (it will have adverse consequences on the wider adoption of emerging business models and related technologies): instead, they should be equipped with the necessary knowledge of how they should tread the information highway.

STR2. Public consultation for the perception of privacy in the digital age will be helpful in outlining the data protection requirements, as there is an obvious need to look into the scope of concepts of personal privacy in a networked society. Like the perception of security, it is different among various societies and cultures, and there will be diverse views on the scope and role of privacy. However, a dialogue on this issue, together with some programme for educating society about the digital assets, will help them to make informed decisions of their privacy requirements in the digital ecosystem.

Long-term recommendations (H2020 / 2015-20)

LTR1. Development of Digital Business Models to support and promote entrepreneurship in the digital world. These business models need to be more comprehensive than current e-business (or m-business) practices. There are a number of legal and sovereignty constraints in opening up classical markets at the international level. This situation worsens in the virtual world; however, the digital world can provide remedies for these problems by providing better (tamper proof) traceability of actions carried out in the digital realm. This approach will also serve the other objectives of the national policies such as reducing carbon footprints (towards paperless business activities), immigration controls (reduced number of economic migrants as financial opportunities will be available in the digital world instead of some specific geographies), etc.

LTR2. Resilience of cyberspace is indispensable for assuring the business continuity, proper functioning of governments and law enforcement agencies, trust of citizens on these services. Field testing of the cyber infrastructure, contingency plans for the emergencies, training of the stakeholders for unexpected situations, disaster-recovery including secure recovery of critical information, all require thorough consideration of technological landscape as well as social and organisational behaviours.

LTR3. Some evolutionary integration model(s) for the ever-expanding and virtually limitless expansion of the digital world. It is not possible to precisely envisage the long-term situations; however, evolution of the current scenarios in a controlled manner could be helpful in instigating a reliable hand-over to the newer technologies. These models should be able to act like lighthouses, to guide the adoption of newer paradigms such as reaching new heights of data volumes (bigger than Big Data); scalable resources; global dispersion of computing and storage resources, etc.

4.1.2 Global approaches to technical and societal challenges

The digital ecosystem has turned into a cyber-social system, that is to say a dual system with a strong interrelation between a dynamic technology system that offers an ever-changing patchwork of services and a socio-politico-economic system with reactive short loop behaviour. It is urgent to secure both, the value of its components and the value of the brand image of its components, and the value of digital activity, around this system, has become important and essential. It is also important to regulate activity and behaviour to avoid overflows.

Security principles, governing the ecosystem, are based on both technological and social pillars, to make the ecosystem resilient and make use of the system as transparent as possible.

The coming years will be decisive for digital industrial policy in Europe. If users have accompanied the proliferation of digital applications, Europe fell back on itself for the past twenty years, losing its industrial champions and numerous market shares. The objectives of the digital

sector should be ambitious: it is vital in times of crisis, to restore growth and improve competitiveness, to design and produce at lower cost in Europe of high quality products. This is a deliberate policy to define and carry out with determination an industrial roadmap.

The digital sector should be a high priority, supporting digital entrepreneurs, increasing job creation, promoting productivity gains in all areas impacted by digital technology, defending the artists or enterprises that use digital media. This new digital economy will boost all economic activity, improve public services, promoting our culture internationally and will present Europe in the leading ranking of high technologies.

The ecosystem in the world geography

The digital ecosystem is not just a supermarket where avid consumers can purchase goods or absorb free intangible content. The digital ecosystem is a new reign, where entrepreneurs, creators and researchers need to rebuild a new digital era and drive innovation, with rights and duties, consistent with our history. Moreover, the digital ecosystem is not a lawless zone that ignores the existing States, sweeping borders, wiping at the same time justice of the States, despite what hegemonic vendors say (on behalf of the free market, even if it is the law of the jungle) and dominate the Internet or despite what lobbyists say (on behalf of their freedom, even if it encroaches on the other), which are influencing ideology the blogosphere.

If we conceive a new constitution for the digital world citizens, for machines, robots and all virtual avatars that mutate at the speed of computers and travel at the speed of light, the laws of this constitution should be in accordance to the Enlightenment. The concepts of freedom and responsibility of the individuals who command and control these abstract creations of the mind, must inspire legislation on this ecosystem since the billions of events that occur are always caused by a prior action of one or more physical responsible individuals (a user or actor network). These people are located somewhere on the Earth even as it becomes increasingly difficult to locate access (because of the machines to mask identity), a calculation, a data storage or communication because of the mechanisms of virtualization that blur the dates and locations of operations. Lawyers must consider these legal issues (copyright, ownership, access, distribution, etc.) of content that can be cloned by nature and these issues of responsibility for action in a virtual distributed system. Sociologists should analyze the shock of this new digital interaction and mediation with the social world and understand the issues of addiction, digital behaviour and digital social divide. Philosophers should set this new ontology, in its breadth, its diversity and complexity, with its symbolic, existential and metaphysical faces. Linguists and anthropologists should study the relationship between these new usages and new behaviours vis-à-vis the various intricate structures of this ecosystem.

A general reflection on the architectures must be initiated to better understand the opportunities and limitations of this ecosystem, before being sentenced by the alarmist followers outlawing digital gadget and computer fetishists or being hailed by blissful courtiers celebrating wonderful progress of cybernetic society and prodigious innovators. One must not play in excess and discern, in this new digital reign, an inevitable clash as a hubris leading material civilization to certain destruction (companies' click and mortar of the Internet bubble of the 2000s), ground into a digital flour with 0 and 1. There is a conjunction between the shape of the ecosystem, its usage and metaphysical sense. The limits of the digital age will be more visible when the applications of nanotechnology will emerge and when quantum technologies will be mastered, with non Aristotelian logic.

Human values, architecture and usage interrelation

The digital ecosystem is an instrument that must be underpinned by values: responsibility, freedom of expression, rights and obligations of actors (suppliers and users), openness to the world, the transparency aspects public, the desire for progress, knowledge transfer, the requirement of a cyber-ethics. Digital ecosystems must draw from the top throughout the life of citizens and improve fundamental freedoms and the functioning of democracy.

Due to this diversified usage in almost all aspects of our lives, a digital ecosystem cannot be satisfied with a single architectural model: it must allow the coexistence of different models of communication, storage and computing. The ethics of digital media should be maintained so that they can use to change by raising the level of all citizens to a society of responsibility and knowledge.

The world has changed dramatically in recent years regarding the use of networks. An economic rationalization has occurred in high technology. Digital convergence continues slowly but surely. The standardizing move of architectures, formats between telecommunications, computers and television continues and is manifested by a blurring of boundaries between network, computer and storage. We try to make interchangeable services on the telephone, computer and television. While the computer formats converge, devices do not standardize, but diversify and individualize: mobile phone, notepad, personal computer, radio or HDTV. This is driven by the format convergence: standard services and standard formats allow easier integration in different devices; while now the same device can be used for different services, the usage comfort and different usage scenarios call for more adapted, ergonomic representations (eBook reader vs. notepad, notepad vs. notebook, mobile phone vs. laptop, laptop against mediabox, mediabox against gamebox, laptop against desktop, laptop against HDTV).

An ecosystem flexible, simple, universal and polymorphic in its structure, sharpened and adjusted in usage

Computer science is not only a new tool: it is neither a business belonging to service nor engineering. Informatics is the science of organizing symbols and automation of abstraction. All involved technologies, from transistor microelectronics to modelling complex systems, are tangible outcomes from digital science, which took over the mathematical science in its abstract inspiration and fruitful in its application to everyday life and engineer science. Computers and networks are revolutionizing experimental science through the distorting lens of distributed sensors, because the natural experiment under glass was shattered: Galileo's telescope, the still of Lavoisier, Pasteur's microscope were transformed and instrumented as an algorithmic kaleidoscope, at all scales of space-time. Whether one works on understanding the edge of the universe, the origin of the Big Bang, or the quarks and bosons, whether one analyses in real time financial flows, data enterprise that travels over the globe or one organizes geophysical measurement campaigns or collects data on orphan diseases, the observer must slide and stack of thin filter software. When considering the physical reality or human organizations, the researcher and the engineer must conduct an experiment that can last twenty years, the instruments that can cover the entire Earth or be disturbed by hostile rivals in this experiment.

ICT must adapt to new times energy savings. Green thinking must also force the computer to be designed in a world of finitude, by limiting the consumption of energy and paper, reducing polluting components, and the appropriate location of infrastructure for storage and computation.

Europe is characterized by its cultural diversity and historical complexity. The digital single market will not exist until one has incorporated this European specificity (multilingualism, the plurality of interfaces for use, etc.) by a "computer subsidiarity" in the industrial efforts, but also in achievements of the products and services. These two dimensions of diversity and complexity must be considered as an opportunity, not as a handicap against the two other global players (North America and China), where the written language is unique. The modern computer actually allows to juggle abstraction levels (generic, universal) and instantiation (singularisation, individuation), virtualization (heterogeneous remote computer) and incarnation (embedded computing, here and now). Heterogeneity is a natural protection in any dynamic ecosystem. To fill the digital divide, Europe should be able to deploy innovative and tailored services to meet the wishes of users, especially for novices who are struggling to become familiar with interfaces that are too difficult to understand or manipulate.

Strengthen the resilience of infrastructure control and crisis management

Society is becoming increasingly dependent on information technology. Major infrastructures are increasingly fragile and optimized for economic reasons and economic activity is just in time. Therefore, infrastructures must withstand multiple attacks and support many malfunctions. The two phenomena are related since attacks cause dysfunction while the latter are used as situations conducive to attacks. It is, therefore, important to make the infrastructure more robust and resilient. We should also secure critical infrastructures, especially those that are intensively related to digital infrastructure, and essential to the economic and social life.

These facilities are, first, the communication and telecoms infrastructure, themselves. Secondly, these are vital infrastructures such as power grids and transport infrastructures that are widely used in digital networks.

During recent years, critical infrastructures have greatly benefited from technological advances in ICT. This growth has contributed significantly to the effectiveness of these facilities by promoting the automation of certain tasks and optimal use of resources. To make the most of these advantages, these infrastructures, through their local computer networks, are largely connected to the Internet. But the Internet is a public network accessible to everyone, and is also a vulnerable infrastructure, consisting of standard and well known software to most experts. This openness makes all the networks that form the Internet potential targets of many frequent attacks against the Internet and for degrading or disrupting services. Nowadays, computer networks and information systems are a common vulnerability for all modern infrastructures. Also, critical infrastructures are interdependent and the failure of one of them can spread to affect other infrastructures either because these facilities are located near each other or because the interruption of service provided by one of them can cause other infrastructure failures. Given all these factors, it has become ineffective to protect a single infrastructure without worrying about other infrastructures that are interdependent with it.

It is necessary to continue research for different techniques and architectures to improve understanding of domino effects and to fight against the phenomena of propagation of failures resulting interdependencies: propagation simulator between infrastructure failures.

It is necessary to develop a model of interdependencies, generic enough to enable integration of multiple heterogeneous infrastructures while offering the possibility to take into account the main factors affecting the propagation of failures. It is also necessary to find means how to find these interdependencies, that can be multitenant and circular. The involved stake holders do not want to disclose them.

We must deploy probes infrastructure, recording tracks and measures, which must then be correlated in real time to analyse, detect incidents, attacks and failures, and make decisions to ensure continuity of service and reduce risk of deterioration of the system. To prevent cascading effects, then we must secure the interdependencies. We must be able to model and simulate, to analyse the fragility of interconnections and interrelations between these infrastructures.

Finally, this research requires international cooperation to pool methodologies and choice of standards for definition of variables, recording traces and event correlation.

Simulators of infrastructure also require methodologies and common tools to analyse interdependencies and cascading effects of trans-boundary involved now in large international infrastructures.

Governance and digital control, in Europe and worldwide

This ecosystem requires a long-term vision and a regulation adapted to the challenges imposed by the opening of the global market, with a strong axis of our core values of freedom and the permanence of a state of law through a national and European legislation. This is an area where contractors, designers and researchers need to rebuild a new digital era, with rights and duties, consistent with our European history.

The digital ecosystem is an area of freedom, but is not a wild wasteland ruled by the law of the jungle. It is a cyber-social machine where usage quickly interacts into an open loop on individual and group behaviours. Societal effects should be anticipated.

Regulation must be proactive and should not come always late, exceeded by acquired usage or a fait accompli. Pool regulators of this ecosystem should be strengthened. These entities act more with a desire for independence than in a spirit of collective intelligence at all spatial scales (European, global) and time (real-time responsiveness, long-term vision) and in all dimensions (legal, legislative, industrial, intellectual, cultural).

The neutrality of the entire ecosystem, not just net neutrality

The neutrality of the ecosystem (the communication function, but also the storage and computation functions) must be established so that all stakeholders and users can fully exploit, seamlessly, the resources of this ecosystem: the network, but also server farms or content farms.

Access to the ecosystem, and all the features and capabilities of infrastructures need to be fair, so as to reduce the imbalance of access and means between rural and city locations.

Technical stagnation has led us to a world ruled by the law of the jungle of applications on globalized portals, where the value of services and content is pulled down and where the variety of fair and efficient models of communication does not exist. The eviction of the scientific debate has the effect of preserving the best effort model and to recover a weak privacy.

We must ensure that operating a network infrastructure, controlling and using it carefully become a competitive advantage in the market.

The digital multilateral governance at global scale

There remains an obscurity in the management and governance of digital systems: digital management of identity, naming, addressing, filing, and filtering. The scarcity and inequitable distribution of Internet addresses may tilt early or later the global network to a balkanization (breaking up) of the Internet. The current "harmony" of the Global Village may be dissolved into a more brutal confrontation in favour of a medieval landscape, where we will see stand up new protectionist walls.

The governance of global networks must be improved to strengthen the dialogue between East and West, North and South. The Internet governance is taken care of by bodies such as ICANN (Internet Corporation for Assigned Names and Numbers), IETF (Internet Engineering Task Force) and W3C (World Wide Web Consortium). The Internet, aggregates of autonomous systems, needs to be governed by a global, strong, multi-lateral body (or set of bodies acting together towards a common goal).

Integration of national regulatory authorities

In Europe, regulation is divided into areas of expertise. There are so many authorities to regulate the industries dependent on digital domain.

This authority fragmentation does not facilitate the rules of the entire ecosystem. However, given the massive growth of digital convergence, these different supervisory authorities will need to be working so increasingly interdependent; the need for cross-network operation clearly appears to break down barriers, make more efficient and expand reflections of each area of expertise.

In the knowledge society, built in democratic states of responsibility, we must construct an ethic with three components: establishing consent, avoid evil and achieve equity. It is necessary to adapt the legislative provisions in order to address these technical and legislation issues.

Building together a cyber-ethics

The development of a cyber-ethics (rights and duties) is associated with the construction of this new digital urbanization. The digital ecosystem should be borne by humanistic values: responsibility, freedom of expression, rights and obligations of actors (suppliers and users), openness to the world, desire for progress, knowledge transfer, and transparency of public aspects. The requirement of a cyber-ethics should include both dimensions of sovereignty and dignity to promote our values in our countries and throughout the world. Digital ethics should be maintained so that usage can change by raising the level of all citizens up to a responsibility and knowledge society.

The personal and professional lives in developed countries can no longer ignore the ongoing digital revolution in half a century. No need for a user to dominate the art of electronics to watch TV. However, it is best to have some basic understanding of computers to control their personal data moving on the network, in the hands of unscrupulous service providers. Having one computer at home, not connected, is probably not a problem and one can do whatever one wants. But having many applications on the same network requires cooperation rules. Freedom of citizens is at stake. It is the same for companies and States: their computers and their data are strategic.

Digital sovereignty of responsible entities (providers, users) and the redefined responsibilities of access, services, content providers

The concept of digital sovereignty may seem anachronistic in the era of globalization. The embargo threats exist on the data of citizens and businesses: the Web2, cloud computing, data outside the country, operated by an unknown service provider, without any service contract, often without legal representation in Europe, under the aegis of commercial contracts written under foreign laws, contracts that are not valid under European law (see recent attempt to change conditions of use at Facebook).

Aware users (persons or companies) know how to protect their part of their private info sphere, created voluntarily and under their control. However, the part of the private info sphere of individuals and companies, which is beyond their reach and/or recorded without their knowledge, escapes them completely. All their privacy is weakened by a potential intrusion of their info sphere, outside of their control and by a recording of digital traces of their behaviour, which they leave without their knowledge through their digital items, or their avatar in the digital virtual space.

Solution providers will exhibit an ethics, and citizens will have to build a cyber-ethics, to ensure freedom, preservation of intellectual property, and responsibility, with our humanistic values. This is especially for these reasons that we must establish and respect, not only network neutrality, but neutrality of the whole digital ecosystem, by including the retention of personal data and personal calculations. Indeed, we should fight against the indexing of the 21st century that is being done without our knowledge and beyond our control, due to our queries on search engines and following the personal data that are irreversibly inserted in clouds or the huge databases of social networks that are usually abroad, out of our legislation.

The ecosystem can be controlled only if the underlying technologies are and some common sense measures can be considered. In Europe, for 30 years, the legislation is very interested in the data, and not enough software. The law with its notions of finality, proportionality, must be improved in terms of digital modernity.

The digital dignity of users, and respect for privacy and digital behaviour

We must demand that players implement on European territory the principle of digital dignity: not to attack users with unsolicited messages, not to mislead users by corrupting search algorithms with bonus classification according to the funding of advertising.

Users' digital dignity might be trampled responsible if you do not react quickly, issuing rules in the virtual world, rules similar to the principles of the real world, and renewing the tools to prevent and control the ecosystem.

Issues of confidentiality of personal data and the digital behaviour (shadowing, electronic tracing of digital activities and behavioural profiling for commercial purposes) and the development of the filing by calculation become an impediment to development of services. Each person writes, unknowingly, a broken diary, in the records of operators, Internet service providers, websites, search engines, that algorithms can reconstruct with the purpose of inquisition or digital spying, without any legislation.

Digital Industrial Policy

Policy must balance togetherness between “being connected, information, communication, networking and act in a consumer, immediacy and contact society” and “be disconnected, think, design and undertake work for the progress of thought, into organizations with pyramidal hierarchies". This policy must be designed in a sustainable environment, in a society of freedom, with rights and duties for citizens, transmission of knowledge and heritage of European values.

The strength of Europe lies in its intellectual and cultural capital. The export values in the world should be at the core of discussions of deepening and enlargement by the independent construction of a strengthened digital construction to sit in a stable position mastery of these still booming technologies, both in terms of economic terms and our influence on the de facto standards. It is useless to expand and blindly branch out and put all member states on the same level of digital development, before delving into the appropriation structures in industry, government and citizens.

The top down digital approach of a single European framework, which turns on its internal problems of free competition and which varies according to the various countries is not the solution. The pragmatic bottom up approach, by opened to the world, digital entrepreneurs and creators, must also be considered. The rebirth of the digital hope is a leading policy objective, which is a measure of economic growth and for the lives of citizens and all the states.

Restoring confidence

Restoring confidence in the digital construction is the first requirement if one wants to restore the confidence of users, businesses and institutions. The fight against all forms of internal and external cyber crime and internally and externally cyber terrorism should be strengthened.

User’s empowerment goes through users’ awareness of their own behaviour and the value of their digital assets, scattered into various virtual territories (employer, bank, government, access or service providers). Digital assets must be protected against risks of malicious observation and inappropriate destruction and against the opaque exploitation of customer profiling and the use of personal data, without the user consent. One must fight against the untimely international indexing and virtual profiling, which operates through sophisticated heuristics when connecting a social network or a search engine. Indexing through statistic calculation has become more dangerous for the freedom of citizens, as keeping classic filing. The right to capture (digitize a work, photographing an object, event filming, recording in the digital world a good or a work) and the right to forget (erase a document relating to an individual after a certain period) are technically difficult questions to work out. We must therefore devise mechanisms to achieve through a legislative and technical engineering.

Repositioning trust infrastructure at the same level as security infrastructure

Technical security of infrastructure, software and information security is an intractable problem in an infinite, open and anonymous world, where activities can be carried out in total darkness. It is necessary to reintroduce visibility in digital actions. The restoration of confidence with a new clarity in the actions at the light speed for communications and scale of Moore's Law for calculations is essential for the development of the digital economy and the development of the digital age globally. Culture, regional aspects are fundamental in achieving computer trust models. An international debate must take place to instantiate, according to the domains and cultures, trust (and distrust) of nearby users.

The intimacy of private cloud computing

The public sphere is traversed by heavy use of social media: the use of participatory platforms has exploded and their users now are millions. These tools refer to a type of applications embedded in the new Web platforms, including blogs and micro-blogs, online collaborative projects, the social networking sites, sites with content sharing and immersive social worlds. These areas allow the direct expression of users, as a citizen, consumer, but also as more personal views through daily interactions and looking for entertainment or information. Social media thus become centres of information, gaming, contact and communication, but also of cultural expression, identity creation, collaboration, contribution, sharing and exchange of information goods.

Short-term recommendations (FP7 / 2013-14)

STR3. Development of models for global cyber ethics to maintain a smooth stream of social interactions in the cyber realm. The recent past has seen diverse opinions about some high profile incidents (such as Wikileaks, Stuxnet, etc.) where totally different ethical approaches are taken by various segments of society. It is therefore necessary to work out the right balance between the rights, responsibilities, and obligations in cyberspace and its real-world ramifications. Some motivations can be drawn from historical social interaction theory where societies agreed to sacrifice some of their personal liberties to maintain a good societal order.

STR4. Harmonisation of national/continental regulatory initiatives at the global scale as their disparities gives birth to *cyber paradises* where prosecution of malicious activities become extremely difficult if not impossible. Costs and associated risks involved in cross-border compliance activities are simply too much to sustain a business activity across borders. It is therefore important for the governments to work towards unified set of regulations for cyberspace, where geo-political borders are already diminished, in the day-to-day conduct of business and commerce. These must address the possibilities, in the event of trouble and dispute, for legal loopholes and jugglery that could overwhelm the stakeholders.

Long-term recommendations (H2020 / 2015-20)

LTR4. Establishment of some universal trust models where users will have suitable means to develop trust relationships based on communities. Both virtualisation and mobility complicate and exacerbate trust establishment metrics. Furthermore anonymization leaves almost no space to develop a critical mass for establishing trust. The universal trust model will need to address this catch-22 like situation where stakeholders of digital ecosystem will be able to establish trust without disclosing too many details that may then compromise their security and liberties.

LTR5. It is necessary to develop some suitable digital governance model with necessary powers for the governors. This is not a trivial task, as any centralisation is either not welcomed by the countries, or their limited scope makes them an ‘advisory board’ whose advice can never be a legally binding verdict. It is therefore necessary to first establish the “added-value” of having such governance that could be helpful in encouraging different stakeholders of cyberspace to work under this protective umbrella.

LTR6. Technological support to achieve digital credibility will be the cornerstone to make the digital ecosystem viable. Trust can never be established if the stakeholders can not find the means to enforce guarantees given to them. The emerging scale of the digital ecosystem together with its complex interactions (including underlying heterogeneity) requires thorough analysis of the technological requirements and the ways to address them. Technological support is absolutely indispensable for translating governance policies and business rules in the practices and operations.

4.2 Network and Information security / cyber security

The ICT landscape has been transformed and expanded in recent years, giving rise to the expansion of threats and vulnerabilities also, and the international security community must come together to deal with this major challenge.

The rapid deployment of ICT and the growing availability of services provided through cyberspace to a very large proportion of world population (of 7 billion individuals there are about 2 billion Internet users and 4 billion mobile phones), raise questions in terms of security and safety of goods and people, but also businesses and institutions. Traditional ways to be informed, to share, to communicate and express, to organize, to consume, to learn, to play and to entertain and to be entertained, are upset by this digital invasion into everyday life. New usages emerge such as contact and immediacy tools provided by Internet of Things, pervasive social networks, blogs and micro-blogs.

The divisions between the two spheres of public life and private life – individuals and organisations – have been altered, if not shattered. The new usages and the emergence of a global space with a virtual freedom where everyone can learn, meet, collectively communicate, display ideas, exchange information, deliver opinions, influence, are blurring the whole social sphere and disrupting the traditional functioning of nation states. These new services are even interrupting sovereign institutions of the security of nations, causing them to discover, explore and monitor these digital areas with totally new approaches.

4.2.1 Evolution of threats and vulnerabilities

Despite the many opportunities and the obvious benefits of modern development of ICT, digital technologies bring with their usage ominous threats of intentional attacks against cyberspace, with the goal of massive indiscriminate targets, or specific targets, to affect citizens, consumers, businesses, institutions, banks and even states. They also sometimes reach the image or the dignity of persons or businesses, by personal attacks (media lynching, misinformation, rumours, mobbing, bullying).

Also, digital threats have continued to evolve over the development of networks and the Internet, and not only have the characteristic to adapt to new security features, but often anticipate them, as the whole complex Internet infrastructure is quite fragile in its design and operation mainly due to the rapid evolution of ICT, While the components are increasingly sophisticated, there is a persistence with older technologies.

All critical infrastructures are interconnected providing accessibility to anyone, anytime. Thus, all these infrastructures are vulnerable to attacks, but also to failure because these constructions are rapidly evolving. They have little protection as they are often left open and interconnected for easy and widespread usage. Therefore, they cannot be protected by the classic means such as access control and authorizations, since users are already “inside”. Or rather there is no inside/outside. Their security also relies on conventional security technologies, often obsolete or at least out of breath. There is also the prevailing culture of proprietary and formerly closed, separate system thinking. This culture prevents the involved manufacturers and the concerned operators to disclose vulnerabilities, flaws, etc., which continue to exist in obscurity.

Cyber attacks on certain industrial infrastructures (chemistry, water supply, traffic or air control, defence systems) could lead to loss of life and property. Indeed, a computer malfunction in one of critical areas could indirectly kill people, or lead to ecological disasters. With this in mind, it is important to prepare for massive failures or potential attacks on critical infrastructures, or the concurrency failures during massive attacks, or attacks during outages.

Crime and terrorism have captured these new modern media and use the digital medium, in general, so commonplace to communicate, share, make themselves known and to recruit. Cybercrime is a direct and constant threat for all users. Vigilance of all stakeholders (users, operators, suppliers) is a necessity. Cyber-terrorism has also become a tangible threat to the reliability of critical infrastructures of countries that are more or less related to digital infrastructures.

Practices of offenders may be local, but in general they cross borders. They are growing across several countries or several continents, mainly to scramble traceability and get around law or tax prosecution in the countries where these attacks are perpetrated.

The inventory of new digital threats is as follows:

- widespread fraud, identity theft and invasion of a offensive marketing, on online advertising, according to an inflation in which greed is perhaps no more the only competitive reason;
- weakening of civil liberties and privacy of citizens by digital filing and spun in virtual communities. A person is no longer sufficiently mistress, or even owner of her online information;
- the considerable evolution of data archiving techniques opens the door to deviant practices implemented by private or public actors for cross-checking and profiling. Memory, without

right to oblivion, beyond our decision-making, legal and territorial control, seems to be constructed, already subject to an organized capture;
- misinformation offensives, verbal abuse, targeted attacks against computer systems to competitors or sensitive infrastructures;
- a lessening of sovereignty of some states, subject to the technology dictate of most advanced nations, even private companies, sometimes adorned themselves of state attributes or delegations.

Threat affects citizens and consumers in their daily activities through the following:

- identity theft and fraud;
- observation and digital behaviour collection and exploitation;
- undesirable content within the reach of children;
- risky practices to varying degrees: online payment, online games, real-time contact.
- threat affects any business:
- intrusion into the information system and destabilization of the company;
- looting of information assets;
- industrial espionage.
- threat reaches even institutions of nations and states.
- out of service continuity and loss of consumer confidence;
- asymmetric low-cost attack and very important "profitability" in terms of impact on shake the entire society.

The digital ecosystem has become a porous medium on a global scale, permeable to all digital flows, with new advents of information storage (cloud computing). Heterogeneous data traffic flows between office, home, individuals and data centres where users store their data. Billions of people are interconnected. Human organizations are dependent on these exchanges for their daily activity. Objects belonging to persons or street furniture are also interconnected.

In their digital lives, people often want to act hidden so as not to reveal their digital activity as digital behaviours leave indelible marks or traces beyond their control. Much of this activity belongs to the digital sphere of work, or is private or confidential. It could be dangerous to display private or sensitive actions (presentation of confidential, private documents, or political opinions), since societal consequences are unknown. It is impossible to hide what is exposed on the Web because there is no possibility of restricting access. One can create private spaces. However, the territories and operation of these private spaces are not organized. Some proprietary applications accept private data, provided that one has agreed to let his personal data in exchange for a free computer account.

The ecosystem has become an unprecedented sounding: Individuals in need of recognition embark on a persistent display or pressure groups involve in discussions with motivations where self-interest prevails over truth. Never before has an epidemic phenomena (distribution of spam, virus outbreak, community behaviour as viewing the same video) spread so quickly.

The private sector has become very important on this scene and expects to intervene and influence the control of system ethics, regardless of the States, by going directly to users, usually less aware or less concerned with the general interest.

The growing unrest and within the ecosystem will be the main vector of future threats. The dispersal and fragmentation of the system components will provide attackers more room to act maliciously. Rather than the entropy of the system, with its complexity, and the incessant movement of active users, the enthalpy of the system, i.e. changes in services and infrastructures, will be predominant in the future for the research community to model its security.

Short-term recommendations (FP7 / 2013-14)

STR5. Study of the threats landscape in an interconnected and convergent digital society. There is more and more interconnectivity of different kind of infrastructures (e.g. electricity power point and data centres; public health information system and commercial drugs manufacturers; etc.). Such levels of connectivity between diverse entities form a convergent system where different kinds of units make use of each other while remaining independent from each other's operational management policies. This convergence together with the complex nature of highly connected systems may give birth to grey areas in the security threats landscape. A thorough analysis of this peculiar paradigm will highlight the security requirements of future security functions.

STR6. Investigation of the readiness of operational critical infrastructures to respond to the emerging threats. It is observed that the security of the critical infrastructure generally relies on physical security and together with security by obfuscation. However, the readiness to respond to remote ICT-related threats and to ensure resilience is hardly tested. The near-total dependence of entire societies on these infrastructures implies that an investigation of their operational readiness to deliver minimum services in the advent of some successful attacks will help the policy makers and solutions designers to properly address them. Keeping in mind the critical and sensible nature of such investigation, the scope could be restricted to authorities.

4.2.2 Threats and vulnerabilities in the years 2015 – 2020.

The security research community within H2020 must deal with a significant change in threats on the digital ecosystem in the coming years (2015-20). This qualitative change will occur following several major developments:

The digital ecosystem extends its power and prerogatives. All fields of human activity are dependent on the digital industry. While it was in the 2000s, a tool for communication and consumption, it becomes increasingly a tool for displaying opinions and ideological views which have taken over all segments of society and all areas of human activity. Digital is an extension of man: the computer is neither a tool nor a service; it is a kingdom in its own right that is changing at its own pace and decreed its independence.

The exponential increase of traffic with data flow and computer programs has organized uncontrollable chaos. Advances in optics allow data rates of the order of Terabits/s in large arteries and the deployment of broadband wireless cellular networks allows downloads of several Megabits/s. Intercontinental flow and data flow grow similarly. The velocity and frequency of spreading viruses and spams follow the same trend. Network denial of services and network wars on a continental scale are not sufficiently studied.

Interconnection which is constantly becoming easier between wireless and wired infrastructures allows anonymous abuse, the source of fraud. Mobility will increase anonymous attacks.

The rise of private sector in computer resources takes away the power to government agencies. Large multinationals have more computing power than large western States: digital sovereignty is no longer assured, except in a few states. The professionalization and internationalization of cybercrime have greatly expanded.

The proliferation of actors in the ecosystem functioning blurs the mapping of the chain of responsibility. The division of labour, more and easier, allows circumstantial alliances.

Cryptography that was the prerogative of States and governments becomes a tool of empowerment for users and groups who use it to circumvent the laws of governments. The attacks of the future will look like great plates of calculations that will move dynamically, anonymously and

furtively in the ecosystem. With the evolution of digital technology, new attacks will appeal to more distribution mechanisms and more strike force in the effects. The future attacks will be the type of opportunistic networks, i.e. individuals or groups of individuals who are ganging up spontaneously and temporarily, to attack a site. Due to the networked interconnection and globalization, the protesters' movements gang up without necessarily having a common history; ideology plays more: alliances, sometimes against nature, appear to fight against a multinational, a bank, etc. The power belongs to consumers. The distribution of tools (database, computer programs) helps them a lot.

The propagation emergence of rumours, vilification and defamation of individuals, institutions or states, the increasing attacks in the open on media targets has gained major importance on the internet, for good and bad reasons. It is also the emergence of protest movements that use the ecosystem openness with borderline behaviour (Anonymous, Wikileaks) or outright in crime. Internet has become a sounding board for asymmetrical confrontations, using the speed and display capability of the network from its weaknesses of legal response: not validated, not authenticated information may be devastating for an individual or a company. Internet has become a playground for activism and lobbies that shape opinions over-react or spread rumours.

The emergence of the powerful web players that can interrupt their service in order to put pressure on the law of a State.

In order to counter future threats, a perimeter security, under the responsibility of each user, is no longer appropriate. It is important to early detect these attacks upon entry into the network or inside the network, which these are due to mafia organizations or governments.

Protection of an ecosystem must appeal to new concepts. It is, therefore, necessary to define new security models that fit into the new communication models. It is necessary to bring closer communication models and security models, so that security becomes an intrinsic property of the communication function. Regardless of the data flow, it is important to implement a sensor network connected to the routers so that these sensors can account for some statistics (offline but rapidly) in response to an attack. The deployment of this local information network (which will have its own tight communication network while borrowing the same physical network as the user data), will help to proactively respond to anomalies within the network.

Compliant with the intelligent terminal paradigm, the principle of the Internet adopts the enforcement of a security policy at the ends: the terminals (smart phones, PCs, tablets) have firewalls, antivirus software suites to thwart security threats from the network. This security, which protects each user, is supposed to reduce the spread of network attacks. This is a perimeter security. Telecoms operators secure their infrastructure with tools related to the security of information systems. It is also only a personal security. It means that it must be re-done hundreds of time, very inefficiently.

It is necessary to gather the chain of communication actors, if one wants to improve Internet security. The user is not alone on the network, he has "friends". The telecoms operator is not alone to operate its network, since he has "friends" and actors (service providers, network actors) that can help in the search for better protection on the network.

Long-term recommendations (H2020 / 2015-20)

LTR7. Data ownership rules need to be renegotiated as more and more data is stored in cyberspace, accessible to a range of different actors (public as well as private); however, the controlling of the processing of such data (of personal character) requires redefinition of data ownership rules in these cyberspaces as otherwise without proper responsibility of a data owner; and/or without any means to control the use of data by its controller, the result will be chaos. Moreover, any loss or corruption of such data will have irreversible consequences on the protection of personal lives.

LTR8. An emerging security issue is to manage panic among the population in the advent of any major disaster arising from ICT. Citizens rush to the ATM machines even if there is a rumour of financial collapse of a bank, let alone an economy. We need to develop contingency plans to avoid alarm in the case of any high profile cyber incidence (including how to manage the circulation of rumours of 'cyber collapse'). With the propagation of information with the speed of light, it is impossible to match the pace of rescue staff mobility with the pace of information diffusion. The task of crisis responders becomes huge in the face of panicked members of a community.

LTR9. With the ever-increasing volume of data and information flow across sites, it is necessary to develop new traffic management models to deal with 'rush hour' flow management especially in the advent of emergencies. These models need to guide the different stakeholders of a digital ecosystem about the modalities of using communication channels in the advent of an adverse situation as well as providing good management of the underlying communication infrastructures for routine operations. Account should be taken of new traffic demands and patterns from the world of (IoT) 'things' that will have different behaviours from human-related Internet usage.

4.2.3 The fight against cybercrime.

Users do not trust computers. ICT seems to them opaque, even hostile: hard to use, we never know if the exchanges will be fine. Consumers have only a relative confidence in the payment networks: spam, virus, limited confidence, fraud, cybercrime (with online payments). The electronic signature does not spread despite European directives and laws. If secure communications are a settled issue, this does not even content distribution and / or services online.

The fact, on the Internet, to be in contact with each other through writing creates anonymity, therefore mistrust. Moreover, this anonymity is sought by some users of dating sites, forums. We never know who is at the end of the server, unlike the telephone, where we recognize the speaker by his voice, or when you are aware of its ability to respond to requested information when you go to a one-stop service public. If we want to promote electronic commerce and enhance online services, we must fight against identity theft, fraud, crime, money laundering, computer misuse.

In a globalized and violent world, the mark of our values, defence of our principles and our model should guide our action to healthy organize digital information intelligence and protect independence, sovereignty and integrity of digital assets of citizens, businesses and countries.

This is a social issue to facilitate the use of ICT and to fight against the digital divide. The challenge is to establish or restore confidence in the digital world to increase e-commerce, intangible trade, e-government, and even the e-republic.

A digital society has the advantage of spreading further and faster knowledge, provided that this knowledge is disseminated and not embedded in the flow of information, disinformation, in informational waste that is distracting attention. We must promote a smart society to create intelligent jobs with smarter products and services. We must instil trust into information with crosschecking sources, and separate views from information.

Beyond the digital divide, as the tree hiding the forest, appear the social divide (financial), that of age (as our populations age) and the territorial divide.

Short-term recommendations (FP7 / 2013-14)

STR7: Initiatives for the creation of digital security task forces at national, continental, and international levels with clearer distinction of the roles of different actors such as CERTs, FCCU (Federal Computer Crime Units), Intelligence Agencies, etc. These actors may require further complimentary units. However, they need to be woven into the fabric of the digital security ecosystem with clear allocation of responsibilities.

STR8: Towards legislation to facilitate the use of digital evidence in courts of law. Having concrete legislation in the short term is not a realistic objective. However, taking early serious initiatives to facilitate the preparation and consequent adoption of such legislation will be an important milestone. The preparation phase will require a multi-domain approach to resolve technical issues (especially the soundness of digital evidence), legal issues (acceptability of digital evidence without compromising the social rights of citizens), policing issues (how to collect and preserve evidence in a 'virtual world'), etc.

Long-term recommendations (H2020 / 2015-20)

LTR 10: User awareness programmes need to be developed for different but overlapping groups of society. These programmes need to be tailored for each community (elder community, teenagers, illiterate people, etc.). The best defence against cybercrime (as for any other kind of crime) remains 'prevention' – prevention is better than cure.

LTR 11: The cyber world is considered as a space with no borders. However, demarcation of responsibilities for cyber-protection will require some distinctive boundaries for the various agencies and departments that will be different from geo-political borders. Therefore, there is a need to develop cyber-policing rules including virtual border-controls in the digital world. The stakeholders of digital ecosystem should be aware of the entity that is responsible for the security of their digital assets. It could be transparent for the users (similar to 112 emergency number in Europe).

LTR 12: Cyber defence can never be effective without having an international dimension. Developing modalities for international cooperation for cyber security is the cornerstone of global security of digital ecosystem.

4.2.4 Cooperation in cyber-defence against the asymmetric challenge.

Cybercrime has changed its status in recent years. It became a true underground industry in the margins of civil society. Cybercrime is the set of criminal offenses likely to be committed via communication networks, ICT being the target of the offense or the means by which it is committed. The venal action, the financial gain is the main goal of cybercriminals. Violations, including those of privacy, are only the means to achieve it.

The action of power, the pursuit of power over others (individuals, groups or states) is also a more widespread goal (control of information, misinformation, revenge, libel, denial of service).

Organized crime has appropriated and organized this new market that enables it to achieve its internationalisation at minimum cost and risk. Geographical specialisation is emerging.

An underground economy with the marketing of goods and stolen data, malicious software, tools, expertise and talent was born in parallel with the traditional economy.

They are hacking tools, development of malware, botnet construction, in a first phase, identity theft, the collection of personal data and / or financial data, in a second phase, online banking attack, electronic commerce attack, in a third phase, and finally the establishment of a network of cyber-laundering and transferring of illicit gains. There is a market for vulnerabilities, malware and botnets.

The threats to businesses and citizens are threefold:

- the unavailability of the service (paralysis),

- damage to sensitive or strategic data, and
- damage to the image (disinformation, defamation, loss of friends or clients' confidence).

Protection of marketable data has become a vital issue, because of the endangerment of business confidentiality and competitiveness, and increasing the legal liability of companies and even now citizens (compliance, traceability and confidentiality).

It is important to strengthen international cooperation in research on cyber-defence, by mapping the attackers, their motives of gain or destabilization of society, and on the cycle of activities of cybercriminals.

All countries are affected by the scourge of cybercrime. Cooperation on security research is needed to anticipate new threats and new vulnerabilities that attackers use preferentially. Cooperation can develop interoperable tools and methods to anticipate and detect attacks in the core of the network and to counteract the effects on usages.

Compatible observation and alert systems at all levels must be deployed to effectively fight against organized crime.

Short-term recommendations (FP7 / 2013-14)

STR9. The number of corporate disputes resulting from claims on digital assets is on the rise. A framework for dispute analysis of digital assets will not motivate stakeholders to take cyber revenge, as there will be a better outlet to resolve corporate disputes in a more logical way without harming the security of their rival's digital assets.

STR10. Mechanisms for responsibly sharing data on cyber offenders' will help other stakeholders to be aware of the potential attackers in their surroundings. This approach will also deter the potential future cyber thieves from their actions as it will cost them far more than what they might have gained in the shorter term. It will also help policing the cyber territories by the respective units.

Long-term recommendations (H2020 / 2015-20)

LTR13. A global virtual space without borders provides an ideal location for criminals to hide themselves while persistent connectivity enables them to remain in contact with their partners in crime and with potential victims. An effective anti-cyber laundering initiative will deter these criminals and help authorities to identify new kind of attacks and frauds.

LTR14. Development of suitable audit mechanisms for a virtual world is something unthinkable until recently. However, the emergence of virtualisation technologies and their use by mission-critical industries require a corresponding set of monitoring and auditing techniques for virtual infrastructures that can provide reliable testing of the effectiveness of security capabilities of these infrastructures.

LTR15. Post-incident investigations are very important to analyse the perpetrators of digital crimes and to prosecute them for their activities. These digital forensics analyses are still not truly adapted to the virtual world of the digital ecosystem. New methodologies and tools need to be developed to meet the requirements of performing digital investigations of cyber world. These new techniques need to consider the peculiar characteristics of virtualisation of computing and storage resources besides globalisation of criminals and their targets.

4.2.5 Protective measures of defence and deterrence.

The technical, legislative, organisational countermeasures to prevent, detect and react against such potential threats (attacks or huge failures) exist but are not worth the trouble. The pace of technological change (extension of the deployment of digital infrastructure, increase of data flows on networks, emergence of innovative services) and the always higher rate of usage change should

prompt governments to continue their efforts in the research field, in the short term but also long term to reduce, if not overcome these dangers.

Digital security becomes increasingly important in science and technology, research programs, accompanied by sociological and psychological usage studies on benevolent and malevolent behaviour on networks.

Each nation has its legislative program and its research program to fight against cybercrime. Countries have implemented various strategies including security measures, covering both defence and deterrence: measures of defence when it can cope with these failures or attacks, but deterrence when technical measures, alone, are incomplete or ineffective (fight against illegal downloading, for example). However these strategies are ineffective when attacks come from abroad or when exchanges are beyond geographic boundaries. Any national policy is very insufficient to defeat cyber attacks. Attackers are also the first to imagine such tactics to divert the laws of a country.

Technical measures alone are insufficient because it is very difficult to prevent failure and / or attacks. Detections are not early enough. The defence measures are still incomplete. However, methodologies for recovering from a situation, following damage, have improved significantly.

Cyberspace is global. The generalized interconnection of digital infrastructures removes the borders of these networks. Interdependence and the porosity of information flows between nations and continents are significant. Only a proactive international cooperation can effectively fight against these issues that could lead to disasters in areas of varying degrees, across a region, country or continent.

Moreover, several virtualization technologies tend to erase the notion of physical space. It is nowadays difficult to know the actual storage location of a file, the location where the calculation is performed as well as routes and the crossed areas through a communication. A file (see P2P technology) can even be piecewise stored in several different countries. A calculation can be performed in two different continents and a communication can take place on very scattered roads.

Furthermore, in terms of the acts themselves, the respective authorities of different countries qualify differently certain offenses. The terms of cybercrime, cyberterrorism are themselves differently understood in different countries. The international community has not yet been able to agree on the vocabulary and basic concepts.

International cooperation in the fight against cybercrime is essential if one wants to limit failures and attacks on cyberspace, maintain stability of services on infrastructures and encourage society development with digital technologies.

The focus must be on the international legal measures to establish a tranquil state on these spaces and in real time exchanges, to detect and prevent propagation of faults. Measures should also allow the data exchange to analyze cybercrime and share experiences.

Short-term recommendations (FP7 / 2013-14)

STR11. The first step towards the readiness of nations to deal with cyber threats is to maintain a credible level of cyber deterrence. Governments should conduct/facilitate targeted and specialised consultation on the concept of cyber deterrence and its impact on the global security landscape.

STR12. It is observed on a number of occasions that political manoeuvrings often use deterrence as a threat or a negotiation chip to settle issues. It is therefore necessary to analyse the scope and overall impact of cyber deterrence in the emerging geopolitical landscape of the world politics.

Long-term recommendations (H2020 / 2015-20)

LTR16. A number of countries may require legal or even constitutional changes to erect cyber deterrence. It is therefore necessary to first develop the framework and modalities including legal and constitutional implications for cyber deterrence. There may not be a single framework for each country; however, countries can use the basic model as a reference to implement it in accordance with their own priorities and sensitivities.

LTR17. The implementation of a cyber deterrence framework will require adequate support for the technological developments to achieve the operational control. Without policies and tools to enforce these policies, the practical side of this framework will never be achieved.

LTR18. Training of the stakeholders involved in the digital ecosystem requires regular cyber defence exercises. In addition to updated training, these exercises will also provide opportunity to identify the shortcomings; and to stimulate the research activities to address them.

4.2.6 Cloud computing security companies.

At the 18th DEFCON in October 2010, 96% of pirates who were consulted said that cloud computing was offering them real opportunities, some have even likened the latter to a weapon of mass destruction.

The virtualization technology used extensively in cloud computing to reduce application complexity and to simplify usage leads to serious security issues: the client or the consumer no longer knows where his processing is based and where his data are stored. The business heritage is located outside the company premises, outside of the country.

The major problems of cloud computing are outsourcing risks condemning a passivity while the dependence does not exempt from responsibility. Distributed storage areas, scattered jurisdiction and the loss of physical control of data give rise to risks related to governance and territoriality. The reversibility of choices is uncertain, so this risk requires a strong need for contracting.

In traditional outsourcing, contracts are stable (licensing, outsourcing, hosting), their legal status is granted and the case law is fairly well established.

However, with cloud services, contracts are more complex (service level agreement, reversibility, territoriality, guarantees) and there is still no real precedent. Legal expertise is essential to a better basis of contracts, which will ensure compliance, quality and continuity of services and data security.

Research of international harmonization is necessary if we are to secure cloud computing with user education to digital risks and to their personal responsibilities, and building a law dedicated or better enforcement of existing law. We must secure cloud computing and more generally virtual resources. Security of information irreversibility is the most crucial point to solve.

Short-term recommendations (FP7 / 2013-14)

STR13. Investigation of the scope of *Cloud danger* to provide a pragmatic view of the opportunities vis-à-vis the vulnerabilities of this borderless computing paradigm. Some stakeholders are simply denying (or overlooking) the prevailing extent of cloud security concerns; whereas others are too sceptical to take full part in cloud-centric opportunities. It is therefore necessary to look on the both sides of the coin and to make informed decision on the basis of the facts instead of hypes and beliefs.

STR14. Like any other business activity, cloud-based business infrastructures will eventually have to come within the net of regulations. The readiness of these infrastructures and the costs of operating these infrastructures require a thorough analysis. Therefore, impact of regulations on the cloud business model needs to be evaluated as it is possible that the management and operations of cloud infrastructures with the full burden of regulatory control will no longer be a viable solution for businesses, especially for SMEs.

Long-term recommendations (H2020 / 2015-20)

LTR19. It is necessary to develop some sort of 'operating permit' to cloud service operators. The issuance of such authorisations will require some controls to be carried out so as to verify that operational functions (including security) are put into practice. It is therefore necessary to develop suitable security audit of best practices for cloud infrastructures. These best practices will also pave the way for a sensible set of cloud operating regulations.

LTR20. The flow of data and information across the geopolitical borders in the cloud paradigm will require some sort of global data and information flow agreement to facilitate not only the export control but also help in identifying and apprehending the digital culprits. There will be obstacles to agreeing universal definitions; however, like global navigation treaties, it can be achieved by taking all the stakeholders on board.

LTR21. Like any other business activity, the use of cloud computing will have a number of risks that its stakeholders have to manage at various stages of their activities. It is therefore necessary to develop risk metrics for cloud usage for individuals, for businesses, and for administrations, so that they can use appropriate risk management techniques for their specific usage needs.

4.3 Programme /funding focus/ identify community

Global alignment, consensus and outreach of the visions and challenges of all the participating countries

One of the areas being looked at by WG 3 is how to move from a more tactical based approach (bi-lateral) towards a more strategic approach (multi-lateral approach). For 2013-2014, it isn't clear how this can be accomplished with the current mechanisms that focus bi-laterally on seven (7) regions. While this regional approach may work for higher level themes, the main difficulty arises when a particular research topic, for example, cyber security, needs to be addressed globally and multi-laterally amongst many regions and the bi-lateral approach is not suited for this type of longer term strategic activity.

Short-term recommendations (FP7 / 2013-14)

STR15. The Commission should engage with fellow programme management and research communities worldwide to engaged in international cooperation to gain their insights on how to move to a more multi-lateral strategic level approach in the future.

Long-term recommendations (H2020 / 2015-20)

LTR22. Strategic global frameworks or approaches should be enabled in the H2020 funding mechanisms for multi-lateral cooperation.

4.4 The relationship between Europe and emerging countries

Digital security has become a growing concern in all countries. In developed countries, all industrial activity and the economy depend largely on digital infrastructure and social and daily life of millions active people is punctuated by the use of digital services. In the emerging countries, the concern is also of concern because of the strong dependence between the effort of economic growth in these countries, confidence in the education of the population for digital usage promotion and deployment of digital infrastructure.

Short-term recommendations (FP7 / 2013-14)

STR16. With the ever increasing and irreversible pace of the digitisation of the activities of modern daily life, it is important to facilitate the development of dependency metrics of digital ecosystem so as to evaluate their impact and due diligence to protect the functioning of routine government and business affaires including lifesaving and mission critical operations.

Long-term recommendations (H2020 / 2015-20)

LTR23. It is important to be prepared for any adverse situation in the same way, say, that citizens are trained to cope with a nuclear disaster. All the stakeholders in cyberspace should know how to behave in the absence of, or prolonged interruption to, digital space; and how to minimise the impact on their daily lives. It is therefore necessary to develop contingency plans and exercises to cope with the aftermaths of a possible outage or serious depletion of digital resources. Global cooperation in this regard may help us to be able to have access to some minimum, possibly stand-by, resources outside the disaster zones that could be accessed via satellites to manage recovery and restoration operations.

4.5 Regional Agreements

Digital networks are essential to the life of countries. Country activity increasingly depends on information technology. To protect vital interests, these countries have addressed the security organization, taking national legal measures. But without international cooperation and without pooling of knowledge and information on crime, national measures are insufficient, sometimes even powerless. Even agreements and partnerships across a region or a continent are not effective, because access or origins of attacks can come from anywhere on the planet.

Traditional markers of country security are scrambled, and it is necessary to work on a different scale of time, space and effort.

Short-term recommendations (FP7 / 2013-14)

STR17. It is important to establish priority-management models to facilitate the sharing of critical cyber data and information with peers at the global scale. Normalisation of the parameters of these models will be problematic as they will be of diverse nature such as political, sovereign, structural, etc. However, a dialogue is necessary to make a right step in the right direction.

Long-term recommendations (H2020 / 2015-20)

LTR24. Any cooperation initiative also results in difference of opinions and approaches that often lead to disputes of variable severity. It is therefore recommended that while fostering global cooperation in the area of cyber security, it is equally important to develop a global digital dispute analysis and resolution framework to resolve conflicts among the participating entities.

4. Conclusions

The need for an international, global extension and for cross-discipline collaboration has become more urgent during the last decade. An international vision of the digital security is essential because the ICT ecosystem is a continuum, a territory without borders, where the laws of any country are increasingly difficult or impossible to enforce.

A multidisciplinary vision of digital security is also important because the ecosystem is a cyber-social meta-system, where culture and behaviour are different depending on socio-economic situation, context and country. It is therefore necessary to bring together all relevant disciplines – technologists, lawyers, economists, criminologists, philosophers, linguists, psychologists and sociologists – if there is to be a holistic framework that can span all the cross-cutting issues.

5.1 Future research challenges for international cooperation in trustworthy ICT identified across the BIC Working groups

The goal of security research is to strengthen the resilience of digital infrastructures and combating cybercrime and cyber terrorism, and all forms of malicious actions of a future in the years 2015-2020. Resilience is an obligation to prevent the devastating domino effect into the open and interconnected networked world. Crime adapts to new usage and is moving towards ubiquitous tool of the Internet and mobile phones, which is faster, more efficient, and more anonymous than the actions in the real world. Cybercrime opens to new digital practices of citizens. It is growing and becomes blight on the growth of the digital economy and human progress. Cybercrime is a dark component of digital trade globalization.

Communications are nowadays protean and attacks inside the network can have as the main vector some forms of communication that does not require access or knowledge of its contents. Operators can no longer declare themselves deaf and blind to the form of communications.

Future international threats are many: identity theft, anonymous mailing, transnational illegal sale of fraudulent or counterfeit products, software, database or personal data traffic, counterfeiting, illegal distribution of intellectual or artistic works, violence on branding, financial fraud, guerrillas, corruption, disparagement, defamation, disinformation. The availability of digital service becomes a threat: Wikipedia may close its site 24 hours to protest against a U.S. law.

Attackers are better organised, increasingly fragmented and scattered around the world. They are mobile and have a dynamic power to come together in a stealthy network in order to join and fight for the same target: gangs, organizations, mafias, secret services. In addition, an implicit collusion enables them to associate the time of an attack to unite their strike force. These threats are becoming more apparent on the network. They are increasingly transnational, even transcontinental, in terms of achievement on the network.

There has been a professional specialization in the chain of cybercrime with directory collectors, botnet “herders” i.e. organisers and maintainers, attack tool and directory suppliers, traders and performers. Finally there is an internationalization of the cybercrime chain: collection of potential target identities and manufacture of dangerous software within a country (e.g. Ukraine, Russia), selling cybercrime products and data in another jurisdiction (e.g. Africa, India, Philippines), malicious actions in another jurisdiction in order to make suspect the official services of these countries (e. g. Russia, China, USA).

One should prevent and control these protean scourges of the digital ecosystem that threaten the security of users, consumers, citizens, businesses, institutions and States.

The important security features in a massive world with teeming agitation are essentially accountability: what is the source of an unfortunate event? The notion of memory of what actually happened in the system is fundamental. These pieces of memory are also scattered around the globe. When it comes to states, the situation is as follows: the attacker at the real origin of the attack is also the holder of the necessary logs, proofs. Everybody else will have a hard time to find the real

origin. As it is impossible to identify subjects and objects, traceability of “abnormal behaviours” is preferred to the identity function. It is cheaper not identifying the actions that have no abnormalities, with the possibility of forgetting to monitor the imperceptible attacks of weak signals.

It is necessary to review current approaches. These consist primarily of splitting the various stakeholders (users together, operators together, user and operator, etc.). They consist then to consider the network as a medium composed of opaque pipes that it is prohibited to analyze, and this in the name of privacy of the information content exchanged between end-users on networks. They finally consist to break the digital ecosystem in two separate parts: the area to protect users and the area managed by network operators with the two-faced operator motivation of not being responsible for the form of communications.

Security must cover all areas of networks and applications. The law must define the digital demilitarized territories. Security must use a solidarity principle. All men of good will must unite to share knowledge in order to thwart attacks.

The following topics have been identified during the first year of the BIC project during the Workshops, Annual forum and during the first WGs workshop.

5.1.1 WG1

Human values

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

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

Privacy and Data protection

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

- Who is responsible for the preservation of an individual’s privacy? Is it the government? The corporations? Or the responsibility of the individual?
- How can we as a research community empower the individual to take control of his or her own private data?
- What new powers are needed by the governments to restrain the „privacy violation industries“?
- How can corporations be convinced of the added value provided by privacy preserving services (see the ENISA report on the Monetization of Privacy)?

Data provenance

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

Trust

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

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

Social computing

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

Designing identity management and accountability frameworks

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

Cybercrime

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

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

5.1.2 WG2

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

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

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

New privacy infrastructure, reconsidering privacy spaces, storage function and utensil

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

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

Cryptography

Advanced cryptographic protocols are needed to support privacy and user control in the cloud and in the Internet of things; as these two worlds need to interoperate, key goals are the development of functional encryption, the distribution of secrets to avoid single points of failure, the optimization of dedicated multiparty protocols and the development of novel protocols based on tamper resistance. Cryptography has a key role to play in the developments of privacy-by-design,

and this in applications such as metering, subscriptions, information sharing and data retrieval. A particularly challenging and high-impact application is e-voting.

Mobile Security

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

Software security

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

Standardization and derived metrics

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

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

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

Digital forensics

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

Securing cloud computing for enterprises

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

Initiate green to security

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

5.1.3 WG3

Move from bi-lateral (tactical) approaches to multi-lateral (strategic) approaches

A long term strategy for International cooperation should include a move to a more sustainable methodology for multi-lateral cooperation models.

Complexity, diversity, interoperability of high level models

International cooperation allows everyone to present its architectural requirements, constraints of usage, its legal obligations and technical aspects of infrastructure, in quantitative terms of content, traffic engineering, software platforms, services and usage.

Cooperation will address the coexistence of security models at different levels of architecture and design of new protocols and architectures suitable for different usage.

International cooperation allows everyone to specify together the constraints coming from the necessary network and service interfaces, due to the fragmentation and regionalisation of IT infrastructures.

It allows a high level reflection on interoperability and especially on the security of such interoperability, to prevent contamination or potential corruption of IT frameworks (such as Identity management Frameworks).

Compatibility, interoperability can be resolved at international level to avoid further impossibilities.

Diversity of models, frameworks, designs and implementations

International cooperation allows everyone to describe their own differences, in terms of culture and legislation, and to share the base that unites the various continents.

The diversity of approaches may be geographic (earthquakes in Japan with the need to make robust infrastructures), cultural (in Europe, it must reflect the diversity of linguistic approaches).

Moreover, this diversity is also reflected for example in the areas of health and administration. This has immediate consequences in the management of digital identities and their attributes. Dialogues, and consolidation at the international level, are important to validate the interoperability issues.

5.2 Recommendations

Based upon the bi-lateral workshops, annual forum and working groups activities, the BIC project is in a position to make an initial set of 17 recommendations for the remainder period of FP7 during 2013-14 (Short term recommendations - STRs) and 24 recommendations for Horizon 2020 during 2015-20 (Long Term recommendations – LTRs).

These will be further developed to contribute to the Final BIC Recommendations Report D3.2.

5.2.1 Short-term recommendations (FP7 / 2013-14)

STR1. Awareness raising programmes for general public should be developed to increase awareness and skills in secure use of the digital world. Human users are the weakest link in the security chain. It has often emerged that some security breaches or online frauds could have avoided if users were properly trained. The overall objective of these programmes should not be to make people frightened of the digital world (it will have adverse consequences on the wider adoption of emerging business models and related technologies): instead, they should be equipped with the necessary knowledge of how they should tread the information highway.

STR2. Public consultation for the perception of privacy in the digital age will be helpful in outlining the data protection requirements, as there is an obvious need to look into the scope of concepts of personal privacy in a networked society. Like the perception of security, it is different among various societies and cultures, and there will be diverse views on the scope and role of privacy. However, a dialogue on this issue, together with some programme for educating society about the digital assets,

will help

STR3. Development of models for global cyber ethics to maintain a smooth stream of social interactions in the cyber realm. The recent past has seen diverse opinions about some high profile incidents (such as Wikileaks, Stuxnet, etc.) where totally different ethical approaches are taken by various segments of society. It is therefore necessary to work out the right balance between the rights, responsibilities, and obligations in cyberspace and its real-world ramifications. Some motivations can be drawn from historical social interaction theory where societies agreed to sacrifice some of their personal liberties to maintain a good societal order.

STR4. Harmonisation of national/continental regulatory initiatives at the global scale as their disparities gives birth to *cyber paradises* where prosecution of malicious activities become extremely difficult if not impossible. Costs and associated risks involved in cross-border compliance activities are simply too much to sustain a business activity across borders. It is therefore important for the governments to work towards unified set of regulations for cyberspace, where geo-political borders are already diminished, in the day-to-day conduct of business and commerce. These must address the possibilities, in the event of trouble and dispute, for legal loopholes and jugglery that could overwhelm the stakeholders.

STR5. Study of the threats landscape in an interconnected and convergent digital society. There is more and more interconnectivity of different kind of infrastructures (e.g. electricity power point and data centres; public health information system and commercial drugs manufacturers; etc.). Such levels of connectivity between diverse entities form a convergent system where different kinds of units make use of each other while remaining independent from each other's operational management policies. This convergence together with the complex nature of highly connected systems may give birth to grey areas in the security threats landscape. A thorough analysis of this peculiar paradigm will highlight the security requirements of future security functions.

STR6. Investigation of the readiness of operational critical infrastructures to respond to the emerging threats. It is observed that the security of the critical infrastructure generally relies on physical security and together with security by obfuscation. However, the readiness to respond to remote ICT-related threats and to ensure resilience is hardly tested. The near-total dependence of entire societies on these infrastructures implies that an investigation of their operational readiness to deliver minimum services in the advent of some successful attacks will help the policy makers and solutions designers to properly address them. Keeping in mind the critical and sensible nature of such investigation, the scope could be restricted to authorities.

STR7: Initiatives for the creation of digital security task forces at national, continental, and international levels with clearer distinction of the roles of different actors such as CERTs, FCCU (Federal Computer Crime Units), Intelligence Agencies, etc. These actors may require further complimentary units. However, they need to be woven into the fabric of the digital security ecosystem with clear allocation of responsibilities.

STR8: Towards legislation to facilitate the use of digital evidence in courts of law. Having concrete legislation in the short term is not a realistic objective. However, taking early serious initiatives to facilitate the preparation and consequent adoption of such legislation will be an important milestone. The preparation phase will require a multi-domain approach to resolve technical issues (especially the soundness of digital evidence), legal issues (acceptability of digital evidence without compromising the social rights of citizens), policing issues (how to collect and preserve evidence in a 'virtual world'), etc.

STR9. The number of corporate disputes resulting from claims on digital assets is on the rise. A framework for dispute analysis of digital assets will not motivate stakeholders to take cyber revenge, as there will be a better outlet to resolve corporate disputes in a more logical way without harming the security of their rival's digital assets.

STR10. Mechanism for responsibly sharing data on cyber offenders' will help other stakeholders to be aware of the potential attackers in their surroundings. This approach will also deter the potential

future cyber thieves from their actions as it will cost them far more than what they might have gained in the shorter term. It will also help policing the cyber territories by the respective units.

STR11. The first step towards the readiness of nations to deal with cyber threats is to maintain a credible level of cyber deterrence. Governments should conduct/facilitate targeted and specialised consultation on the concept of cyber deterrence and its impact on the global security landscape.

STR12. It is observed on a number of occasions that political manoeuvrings often use deterrence as a threat or a negotiation chip to settle issues. It is therefore necessary to analyse the scope and overall impact of cyber deterrence in the emerging geopolitical landscape of the world politics.

STR13. Investigation of the scope of *Cloud danger* to provide a pragmatic view of the opportunities vis-à-vis the vulnerabilities of this borderless computing paradigm. Some stakeholders are simply denying (or overlooking) the prevailing extent of cloud security concerns; whereas others are too sceptical to take full part in cloud-centric opportunities. It is therefore necessary to look on the both sides of the coin and to make informed decision on the basis of the facts instead of hypes and beliefs.

STR14. Like any other business activity, cloud-based business infrastructures will eventually have to come within the net of regulations. The readiness of these infrastructures and the costs of operating these infrastructures require a thorough analysis. Therefore, impact of regulations on the cloud business model needs to be evaluated as it is possible that the management and operations of cloud infrastructures with the full burden of regulatory control will no longer be a viable solution for businesses, especially for SMEs.

STR15. The Commission should engage with fellow programme management and research communities world-wide to engaged in international cooperation to gain their insights on how to move to a more multi-lateral strategic level approach in the future.

STR16. With the ever increasing and irreversible pace of the digitisation of the activities of modern daily life, it is important to facilitate the development of dependency metrics of digital ecosystem so as to evaluate their impact and due diligence to protect the functioning of routine government and business affaires including lifesaving and mission critical operations.

STR17. It is important to establish priority-management models to facilitate the sharing of critical cyber data and information with peers at the global scale. Normalisation of the parameters of these models will be problematic as they will be of diverse nature such as political, sovereign, structural, etc. However, a dialogue is necessary to make a right step in the right direction.

5.2.2 Long-term recommendations (H2020 / 2015-20)

LTR1. Development of Digital Business Models to support and promote entrepreneurship in the digital world. These business models need to be more comprehensive than current e-business (or m-business) practices. There are a number of legal and sovereignty constraints in opening up classical markets at the international level. This situation worsens in the virtual world; however, the digital world can provide remedies for these problems by providing better (tamper proof) traceability of actions carried out in the digital realm. This approach will also serve the other objectives of the national policies such as reducing carbon footprints (towards paperless business activities), immigration controls (reduced number of economic migrants as financial opportunities will be available in the digital world instead of some specific geographies), etc.

LTR2. Resilience of cyberspace is indispensable for assuring the business continuity, proper functioning of governments and law enforcement agencies, trust of citizens on these services. Field testing of the cyber infrastructure, contingency plans for the emergencies, training of the stakeholders for unexpected situations, disaster-recovery including secure recovery of critical information, all require thorough consideration of technological landscape as well as social and organisational behaviours.

LTR3. Some evolutionary integration model(s) for the ever-expanding and virtually limitless expansion of the digital world. It is not possible to precisely envisage the long-term situations;

however, evolution of the current scenarios in a controlled manner could be helpful in instigating a reliable hand-over to the newer technologies. These models should be able to act like lighthouses, to guide the adoption of newer paradigms such as reaching new heights of data volumes (bigger than Big Data); scalable resources; global dispersion of computing and storage resources, etc.LTR4. Establishment of some universal trust models where users will have suitable means to develop trust relationships based on communities. Both virtualisation and mobility complicate and exacerbate trust establishment metrics. Furthermore anonymization leaves almost no space to develop a critical mass for establishing trust. The universal trust model will need to address this catch-22 like situation where stakeholders of digital ecosystem will be able to establish trust without disclosing too many details that may then compromise their security and liberties.

LTR5. It is necessary to develop some suitable digital governance model with necessary powers for the governors. This is not a trivial task, as any centralisation is either not welcomed by the countries, or their limited scope makes them an 'advisory board' whose advice can never be a legally binding verdict. It is therefore necessary to first establish the "added-value" of having such governance that could be helpful in encouraging different stakeholders of cyberspace to work under this protective umbrella.

LTR6. Technological support to achieve digital credibility will be the cornerstone to make the digital ecosystem viable. Trust can never be established if the stakeholders can not find the means to enforce guarantees given to them. The emerging scale of the digital ecosystem together with its complex interactions (including underlying heterogeneity) requires thorough analysis of the technological requirements and the ways to address them. Technological support is absolutely indispensable for translating governance policies and business rules in the practices and operations.

LTR7. Data ownership rules need to be renegotiated as more and more data is stored in cyberspace, accessible to a range of different actors (public as well as private); however, the controlling of the processing of such data (of personal character) requires redefinition of data ownership rules in these cyberspaces as otherwise without proper responsibility of a data owner; and/or without any means to control the use of data by its controller, the result will be chaos. Moreover, any loss or corruption of such data will have irreversible consequences on the protection of personal lives.

LTR8. An emerging security issue is to manage panic among the population in the advent of any major disaster arising from ICT. Citizens rush to the ATM machines even if there is a rumour of financial collapse of a bank, let alone an economy. We need to develop contingency plans to avoid alarm in the case of any high profile cyber incidence (including how to manage the circulation of rumours of 'cyber collapse'). With the propagation of information with the speed of light, it is impossible to match the pace of rescue staff mobility with the pace of information diffusion. The task of crisis responders becomes huge in the face of panicked members of a community.

LTR9. With the ever-increasing volume of data and information flow across sites, it is necessary to develop new traffic management models to deal with 'rush hour' flow management especially in the advent of emergencies. These models need to guide the different stakeholders of a digital ecosystem about the modalities of using communication channels in the advent of an adverse situation as well as providing good management of the underlying communication infrastructures for routine operations. Account should be taken of new traffic demands and patterns from the world of (IoT) 'things' that will have different behaviours from human-related Internet usage.

LTR 10: User awareness programmes need to be developed for different but overlapping groups of society. These programmes need to be tailored for each community (elder community, teenagers, illiterate people, etc.). The best defence against cybercrime (as for any other kind of crime) remains 'prevention' – prevention is better than cure.

LTR 11: The cyber world is considered as a space with no borders. However, demarcation of responsibilities for cyber-protection will require some distinctive boundaries for the various agencies and departments that will be different from geo-political borders. Therefore, there is a need to develop cyber-policing rules including virtual border-controls in the digital world. The stakeholders of digital ecosystem should be aware of the entity that is responsible for the security of their digital assets. It could be transparent for the users (similar to 112 emergency number in Europe).

LTR 12: Cyber defence can never be effective without having an international dimension. Developing modalities for international cooperation for cyber security is the cornerstone of global security of digital ecosystem.

LTR13. A virtual space without borders provides ideal location for criminals to hide themselves LTR13. A global virtual space without borders provides an ideal location for criminals to hide themselves while persistent connectivity enables them to remain in contact with their partners in crime and with potential victims. An effective anti-cyber laundering initiative will deter these criminals and help authorities to identify new kind of attacks and frauds.

LTR14. Development of suitable audit mechanisms for a virtual world is something unthinkable until recently. However, the emergence of virtualisation technologies and their use by mission-critical industries require a corresponding set of monitoring and auditing techniques for virtual infrastructures that can provide reliable testing of the effectiveness of security capabilities of these infrastructures.

LTR15. Post-incident investigations are very important to analyse the perpetrators of digital crimes and to prosecute them for their activities. These digital forensics analyses are still not truly adapted to the virtual world of the digital ecosystem. New methodologies and tools need to be developed to meet the requirements of performing digital investigations of cyber world. These new techniques need to consider the peculiar characteristics of virtualisation of computing and storage resources besides globalisation of criminals and their targets.

LTR16. A number of countries may require legal or even constitutional changes to erect cyber deterrence. It is therefore necessary to first develop the framework and modalities including legal and constitutional implications for cyber deterrence. There may not be a single framework for each country; however, countries can use the basic model as a reference to implement it in accordance with their own priorities and sensitivities.

LTR17. The implementation of a cyber deterrence framework will require adequate support for the technological developments to achieve the operational control. Without policies and tools to enforce these policies, the practical side of this framework will never be achieved.

LTR18. Training of the stakeholders involved in the digital ecosystem requires regular cyber defence exercises. In addition to updated training, these exercises will also provide opportunity to identify the shortcomings; and to stimulate the research activities to address them.

LTR19. It is necessary to develop some sort of ‘operating permit’ to cloud service operators. The issuance of such authorisations will require some controls to be carried out so as to verify that operational functions (including security) are put into practice. It is therefore necessary to develop suitable security audit of best practices for cloud infrastructures. These best practices will also pave the way for a sensible set of cloud operating regulations.

LTR20. The flow of data and information across the geopolitical borders in the cloud paradigm will require some sort of global data and information flow agreement to facilitate not only the export control but also help in identifying and apprehending the digital culprits. There will be obstacles to agreeing universal definitions; however, like global navigation treaties, it can be achieved by taking all the stakeholders on board.

LTR21. Like any other business activity, the use of cloud computing will have a number of risks that its stakeholders have to manage at various stages of their activities. It is therefore necessary to develop risk metrics for cloud usage for individuals, for businesses, and for administrations, so that they can use appropriate risk management techniques for their specific usage needs.

LTR22. Strategic global frameworks or approaches should be enabled in the H2020 funding mechanisms for multi-lateral cooperation.

LTR23. It is important to be prepared for any adverse situation in the same way, say, that citizens are trained to cope with a nuclear disaster. All the stakeholders in cyberspace should know how to behave in the absence of, or prolonged interruption to, digital space; and how to minimise the impact on their daily lives. It is therefore necessary to develop contingency plans and exercises to cope with the aftermaths of a possible outage or serious depletion of digital resources. Global cooperation in

this regard may help us to be able to have access to some minimum, possibly stand-by, resources outside the disaster zones that could be accessed via satellites to manage recovery and restoration operations.

LTR24. Any cooperation initiative also results in difference of opinions and approaches that often lead to disputes of variable severity. It is, therefore, recommended that while fostering global cooperation in the area of cyber security, it is equally important to develop a global digital dispute analysis and resolution framework to resolve conflicts among the participating entities.

6 References

[1] Deliverable D2.3 - Interim report of the Working groups activities.
[2] 1st BIC Annual Forum, 29th November 2011 http://www.bic-trust.eu/events/1st-bic-annual-forum/
[3] http://www.syssec-project.eu
[4] http://www.inco-trust.eu
[5] http://www.bic-trust.eu/events/eu-brazil-cooperation-workshop/
[6] 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
[7] http://www.cs.rutgers.edu/~rebecca.wright/INCO-TRUST
[8] http://www.securityconference.de/Home.4.0.html?&L=1
[9] https://update.cabinetoffice.gov.uk/sites/default/files/resources/CyberCommunique-Final.pdf
[10] http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CL=ENG
[11] Remarks at the 28th Annual International Workshop on Global Security, Paris, France 16th June 2011 http://www.defense.gov/speeches/speech.aspx?speechid=1586
[12] 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
[13] London conference on Cybersecurity, 1-2nd November 2011, http://www.fco.gov.uk/en/global-issues/london-conference-cyberspace/
[14] 1st BIC Annual Forum, 29th November 2011, http://www.bic-trust.eu/events/1st-bic-annual-forum/