BUILDING International Cooperation for Trustworthy ICT

D3.2 – Final 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

List of Figures

List of Tables

1 - Executive Summary

The purpose of the BIC coordination action project [1] is to foster cooperation across the international funding agencies and researchers within the focus areas of ICT Trust and Security, in order to understand the activities and planning of the target countries; and carry out a mapping of the European Commission's planning to them, such that a common technical and policy alignment is viable. The building of international cooperation is a collaborative effort that only works if it reflects the views and priorities of the target countries as well as buy-in from the technical experts in the EU along with the target countries.

As shown in Figure 1, Work Package 2 in the BIC project ['Platform for International Collaboration and consensus building'] was responsible for building the INCO collaboration platform of the project which includes the structural components required to provide the high level advisory roles, thought leadership and expertise in the various thematic areas within Trustworthy ICT for cooperation, The INCO platform created in WP2, facilitated and supported a range of activities including the scoping and validating of analysis and findings, the recommendation of potential actions, being a credible interface between the broader research community and programme management as well as acting as 'BIC advocates' and organising local events to broaden the awareness of the project objectives within the target countries. The collaboration platform consisted of an International Advisory Group, supported by three Core Working Groups (CWGs) and a newly formed concept of in-country Extended Working Groups (EWGs) that will carry forward the work after the conclusion of the BIC project. This is the main final report of WP3 ['Input to the design of future research programmes'], which has distilled the findings of the platform via regular workshops carried out within WP4 ['Building the International Co-operation community'] of the BIC project and presents the final recommendations accordingly.

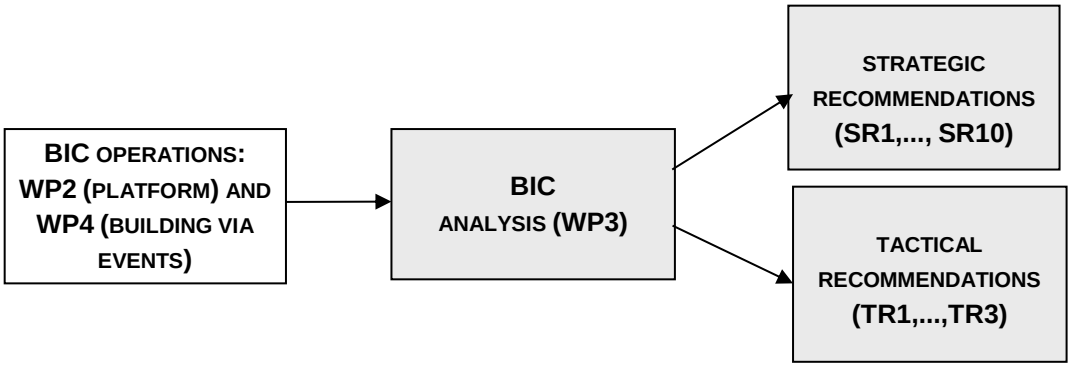

Figure 1. BIC recommendations structure

After an analysis of the bi-lateral activities between each of the countries and further analysis via a survery carried out by the project [2], six priority topics have been identified as a list of potential topics by the EU and Brazil, India, South Africa researchers for mutually beneficial cooperation in the area of trust and security. The six topics are:

1. Cybersecurity;
2. Trust and Privacy;
3. Mobile security, Social media and Cloud security;
4. Security of Applications and data protection;
5. Identity management, accountability frameworks;
6. Future Internet security.

There are developed through two different but related, groups of BIC recommendations, a strategic group and a tactical group, with their specific rationale for inclusion detailed accordingly. The two recommendation groupings, as shown in Figure 1, are not meant to be consecutive, but to address two parallel aspects of the field of necessary international RTD.

- ***Strategic Recommendations (SR)***: setting out the frameworks, common understandings, and overall procedural and governance landscape that takes into account the diversity of social, economic, and cultural norms and requirements worldwide. These can be considered as ground rules and enabling actions that must take place to facilitate effective outcomes of international cooperation in this field in order to carry out the specific (tactical) recommendations.
- ***Tactical Recommendations (TR)***: more specific or concrete research recommendations to progress towards the required technical building blocks and their relationships that will enable a trustworthy ICT ecosystem. Trustworthy ICT is defined as ICT that is secure, reliable and resilient to attacks and operational failures; guarantees quality of service; protects user data; ensures privacy and provides usable and trusted tools to support the user in his security management. It is expected that the newly formed Extended Working Groups (EWGs), in conjunction with their supporting governments and also continued interaction with the EU Commission delegation will also continue to add further to the tactical recommendations in the near future as they continue their work.

The long-term **Strategic Recommendations** (H2020 and 2015-2025) for international cooperation in the field of Trustworthy ICT research and technological development are the following:

1. There is a need for new global approaches, meta-models and methodologies;
2. Global cybersecurity is a moving landscape of attacks, surveillance and failures;
3. International cooperation research is an essential H2020 requirement;
4. The international community must agree on grand principles;
5. There must be a shift in emphasis from the tactical bi-lateral collaborations to a strategic multi-lateral approach;
6. There is a need to keep an international openess in the specifications of services and standardisation;
7. There is a need for an international mobility model approach;
8. There is a need for an international approach dealing with the massive abstraction of software and data (e.g. resilience of virtualisation);
9. An international cooperation is needed to deal with the fragility of interconnections;
10. We need an international approach to steer the evolution and strengthening of the digital ecosystem in terms of network security governance and surveillance.

The **Tactical Recommendations** are:

1. The work of the BIC project, or its structural components (IAG, WGs) should be continued, and expanded to other countries, in the long term;
2. The EU and BIC countries should formally recognise the Extended Working Groups as the nodal in-country agency/body to be called upon for discussions regarding future H2020 (and beyond) international cooperation activities;
3. The EWG should draw up and formalise their terms of references / objectives in synchronisation with one another and get these ratified by their respective Programme Management / Governments.

The definitions, rationale, steps required and suggested roadmapping (timing) information for each of these recommendation are given in the report.

2 - Introduction: Setting the scene on the ICT landscape and its international dimension

The ecosystem around the internet and mobile networks is shaping our everyday lives. It is essential to know the various properties of the relationship between the physical world and the digital world to establish trusting relationships in our relations with others, both in our personal and professional exchanges.The instant connections to the ecosystem have profoundly changed our relationship to information and communications with others, both in our private and in professional lives. Pervasiveness of communication technology and ubiquity of digital infrastructures allows for the constant use of these tools. Exposure of users to this digital infrastructure, still evolving, and the constant fear of being spied on or potential loss of personal data could eventually diminish the ecosystem's image, and consequently change the future architecture of the infrastructure by necessity of barriers, filters and inspections at all stages of usage and operation.

The digital ecosystem transcends borders, and as a consequence attacks and failures are also, at times, trans-border. Domino effects are rare but do exist. This characterstic of the evolving digital ecosystem has weakened the ability of national law enforcement systems of countries to act against trans-border attacks. The local law enforcement is unable to distinguish malicious actions from abroad by an attacker from legitimate activities generated abroad by an honest citizen or a national company who wants to protect its digital assets.The ecosystem involves many players simultaneously at international level. It is difficult to assign blame to an actor, when users complain of a failure occurs due to a fault, an attack or an operating error. Issues of accountability and responsibility are becoming increasingly complex. Issues of intellectual property are becoming more sophisticated. An international and multi-disciplinary vision of digital security is essential because the cyber-social ecosystem is a continuum, a territory without borders, where the laws of any country are increasingly difficult to enforce and where culture and behaviour differ depending on socio-economic situation, context and country. This is precisely why the BIC project from the beginning, has advocated a move away from the bi-lateral approach (tactical) to a multi-lateral (strategic) approach, especially when dealing with international cooperation and trustworthy ICT.

Cyber-terrorism uses the ecosystem as a tool for international communication, as a sounding board to disseminate ideological propaganda and as a means of indoctrination and recruitment across a large territory. Cybercrime exploits networked system vulnerabilities, using the anonymous and borderless nature of trade. Fraud and digital crime, intrudes into the cracks of payment systems by exploiting vulnerabilities of mobility, new equipment, protocols, new operating systems and identity theft (through phishing, etc.). Cyber-activism and hacktivism appeared, because the network is a gigantic means of communication. It has a huge echo, where all information and misinformation are intertwined. Crisis management, due to a failure or a serious security incident, is becoming increasingly important in business and nation states. Both autocratic regimes and democratic governments use external infrastructure, as space surveillance, grafting observation probes and information capture for the purposes of espionage, economic intelligence and the benefit for their national enterprises. They also use the internal infrastructure, as land of policing. Service providers use and abuse their dominant position in relation to the user, being predators of personal

data and privacy, by the collection of personal data outside the remit of their initial goals and operate data massiveness by categorisation algorithms.

The misguided use of some regular users exploits traditional online weaknesses in the system for acquiring music files and videos. All these challenging issues may divert, sooner or later, ordinary users towards conservative solutions, and away from modernity. As our analysis has clearly shown, cybersecurity has become a major issue in all the BIC countries. It applies to all governments, all businesses and all network users, even if the technical measures are not fully implemented to mitigate the risk, especially for small businesses.

Cybersecurity and resilience became the first priority in all industrialised countries and emerging economies. The priorities of research in ICT trust and security are privacy, transparency, for the internet actors (especially for Europe), followed by mobile security, trust, identity management as challenges for 2020, particularly for the emerging countries represented in BIC. Cloud security, intellectual property ownership, accountability, cryptography on digital signature or authentication, are research topics that derive from the these priorities. Issues such as green security, cascading failures of infrastructures are barely mentioned. In Europe, discussions on the Protection of Personal Data Directive reflect the economic interests behind identity management, the mercantile use of personal data, the use of metadata, as well as localisation issues of ICT operations (access, processing, data storage, location of the service operator that manipulates that data). Moreover, mechanisms of identity management (national identity card, access to digital services card) and its attributes (credit card number, etc.), conceal a growing vulnerability in the mobile world in particular. Instead, in the BIC countries of India, South Africa, and Brazil, it has been found that priorities are rather security in real-time from a mobile device.

In addition, a strong emphasis was placed on the need to take into account the culture and history of the country to implement models of trust and reputation in connection with security mechanisms to support e-commerce.The Horizon 2020 Programme will need to take into account this balance between diversity and interoperability on the one hand and usability and flexibility, on the other hand.

While the necessity of comprehensive international cooperation involving -research, industry and government is established, it is imperative that a globally acceptable and sustainable mechanism is evolved that ensures the practical implementation of above philosophy of international cooperation. Towards this the adaptation of the strategic and tactical recommendations (SRs & TRs) of this BIC project report is extremely significant. Particularly, the recommendations on creation and sustenance of the empowered in-country Extended Work Groups(EWGs) and a centralised International Advisory Group (IAG) shall be extremely vital in bringing about the Trustworthy ICT and a sustainable ecosystem for effective cyber security against an extremely dynamic environment of global cyber threats.

In the current H2020 calls, it is not abundantly clear whether this global vision and this global scale is taken into account, as many of the International actions are relegated to the second call for proposals. It is, therefore, essential for Europe to create, at the earliest, calls for proposals in the framework of international cooperation, perhaps starting with joint calls in additional countries, to reconcile points of view, on a continental scale. This deliverable makes an attempt to map the recommendations to the known calls of H2020 and also points out potential gaps in the open calls.

2.1 Everywhere in the world, ICT is the indicator variable of society advancement

The 21st century society relies on digital systems more than ever. Computers are no longer simple machines that are used by organizations or at home. These systems consist of heterogeneous software, hardware, network components of changing capacities, availability, and in varied contexts. Computers became ubiquitous and are embedded everywhere, from smartphones and human bodies to cars or industrial control devices, robots or drones. Moreover large-scale cloud computing providers are sharing them among many organizations in an unprecedented scale. As a result, too often computer systems fail, become compromised, or perform poorly and therefore untrustworthy. They provide computing services to large pools of users and applications, and thus are exposed to a number of dangers such as accidental, deliberate faults, virus infections, malicious attacks, illegal intrusions, and natural disasters. As computer systems become increasingly large and complex, their reliability, security and autonomy play critical role at supporting research, societal and business applications. As computers have become indispensable, their failures and breaches of security may significantly perturb our daily lives. The increased hardware and software complexity, the expending concerns about security and privacy, as well as computer proliferation into new areas, pose new challenges to technologists, sociologists and policy makers. We have witnessed fast development of various ICT in the first decade of the 21st century. At the same time, there has been a tremendous amount of efforts to fuse these individual technologies to provide non-precedent services to the end users. Also, there have been a lot of trials to apply ICT to other industrial sectors such as green convergence, smart appliances, broadcasting and media, mobile convergence networks, and other ICT convergence applications and services, over the various industrial sectors.

2.2 The growing importance of international ICT point of view

Digital snowball still running favourably

For 20 years, the Internet, Web, P2P applications, social networks, cloud computing on the one hand, the mobile phone and the smartphone with its reign of standalone applications on the other hand, not to mention satellite constellations geo-location radically changed daily activity, people's behaviour, and organization and life business. The impact on communication between people in everyday life and in business, on information, on trade and entertainment was decisive and irreversible. Convergence between the world of computers, television and mobile phone is almost behind us. This development and reconciliation also cover all continents. Emerging countries including those involved in BIC are catching up very quickly, and the wider Africa is not absent from this dynamic. The digital divide between north and south, fades slightly. The number of web users is 1.5 billion, the number of mobile phone subscribers is 4 billion. Although Moore's Law is no longer working since about 2009, the digital evolution continues with a feedback loop between practice and technology, at the range of applications. The virtuous circle of development of IT applications continues to turn favourably, and it will as long as there will be no saturation in the various fields of activity. However, there are swathes of new applications to explore into the digital world, including the interconnection of computers with the reality of the physical, animal and plant world (reality support and relay of computer activity) and in interconnection between individuals (massive multi-party societal applications for contact, entertainment, information,

knowledge, collective events), coupled with an analysis of massive data in general (transport, environment, marketing, linguistics, statistics, sociology). The dynamics of this digital machine to produce innovation never stops, and not getting carried away. Despite the constant renewal of the digital set, it has a high inertia, because of the baseline of industrial and lack of training and the ability to change of users, opportunities and benefits outweigh disadvantages. This ecosystem works like a machine that transforms approximately every 3 years, with new services, and a magnet for new usages and new users. Users spend a lot of time in front of screens of TV, internet and telephone. Computer addiction could saturate some adolescents with electronics and computer applications, it would eat like tamagotchi[1]. However, for now society absorbs technology at an accelerated pace, allowing a rapid change. The absorption capacity is expected to slow in the coming years, as various generations have stabilized on certain traditional practices and investments in digital technology settle down to see other new technologies such as nanotechnology, robotics or life sciences.

Reversal: ICT becomes the environment, physical and social reality becomes the content

After computer science in isolation, where computer engineers used to govern the world of computing and where computers were exchanging information with other computers, digital technology has become the medium in which people and businesses plunge and conform to organize their activity. In the last twenty years, computer performance of key functions has greatly accelerated: calculating a factor of around 30, 000, exchanging with theoretical optical bandwidth a factor of around 200, 000, storing of a factor of around 10, 000. Yet if the worldwide web (www) no longer means "wait, wait, wait", transactions are not instantaneous, because they are weighed down by transfer of advertising images, significant email is stuck because of spam, Web sites are filled with bulky videos, so that the working methods do not improve.

The infrastructure is remarkably stable. It does not change, such as IPv4 that is hard to be replaced by IPv6. This continuity is due to the conservatism of the network principles that is trying to evolve towards SDN, particularly for security reasons. One particularly wants to preserve a simple and efficient network. One wants the applications to take in charge and support the different problems, so that the users are responsible. Equipment is naturally renewed every 3 years. It is during these renewals that slight changes occur, paid by the customer. Suppliers become very competitors (Cisco, Juniper, Huawei, ZTE ...). Continental clashes occur with digital sovereignty issues. TCP / IP has not changed in its specifications and in its implementation, but has changed radically in its use. Statistics on the protocol, protocol behaviour, behaviour of applications vis-à-vis protocol, reactions of users facing protocol also profoundly changed. However, there are more and more interconnected people and motivations and interests of such persons or of these companies differ completely. Giants of the internet (Google, Apple, Facebook, Twitter, Microsoft, Yahoo, LinkedIn, AOL, AT&T, Netflix, Comcast), giants carve the lion's share, and predators of personal data, have emerged.

[1] Virtual pet who are given room and we did sleep, and risk of death, if we do not deal with.

In terms of technology, changes are numerous. There are failures, slowdowns, winning developments and success. P2P slowed because it was engulfed in the illegal downloading of audio and video files. The Semantic Web is too rigid, and does not develop: ontologies, algorithms emerging from nomenclature, are not suitable in a still ambiguous world, moving with blurred boundaries. Trust was not instrumented in recent years: the reputation models, recommendation models, frequenting models were not deployed. They are too difficult to establish. Computer activity is a solitary action, independent and in the moment. It does not link directly to the past, always because of blurred identity. Only the digital traces can be used and analysed retrospectively. Collective actions are quite rare on the network. Instant cooperation has trouble finding applications. Yet it is solidarity security applications that could improve the fight against massive and simultaneous attacks as sending viruses or spam. However, cloud computing is booming. Virtualization of computing and storage resources favoured the concentration of storage and computation farms. The network is recursive: while the internet meant a flat architecture of interconnected networks, it is now an interconnection of ICT plates, these plates being fragmented into closed and proprietary subnets, hosting nodes that contain networks of servers. The IP interconnection protocol is pushed, and new forms of routing are under construction: OpenFlow to go faster routing in data centres and information systems, after which MPLS channelled flows belonging to preferred customers, with high priority. The network folds on itself: with cloud computing, a node of the internet network is in reality a true opaque network of anonymous servers that cooperate to achieve their task.

ICT expands along directions of global interest

ICT invests physical reality

The information society is evolving towards a digital society where the physical world will hook to the digital engine. It is the dawn of a world where many devices are connected and will be guided by computer to fill and optimize digital gaps in human activity. The network of billions of phones and computers will drive the 50 individual digital devices at home, for shopping, within cities, during transportation, in health care, which will cause a new scale effect in next ten years. The industry will continue its lifecycle management automation of activities and objects, and organize monitoring and control systems to optimize process control and release sensitive or difficult tasks. The next evolution will, therefore, invest our close environment, further bridging the ubiquity and pervasiveness of the environment. There will be the birth of a systematic interface between reality and us. Our hands and fingers will be used to control, direct actions, give opinions, gather information, possibly calculate, and publish to the whole world. This free display may interfere with the chaotic information landscape and produce a chaotic background noise, where it will be increasingly difficult to extract good useful information.

ICT extends abstract and virtual worlds

But ICT moves also into another direction, far more advanced. In addition to physical objects, ICT creates virtual objects, i.e. abstract, complex entities that rely on other real and/or themselves abstract entities, which may affect reality. These are huge sheets of borderless computations that run across continents, where the notions of finality, location of calculations, storage and communications have no meaning, since the scale of meanings,

actions and responsibilities was deliberately broken. Moreover, the concepts of responsibility and accountability are currently differing on the one hand in terms of real life and human laws, at the scale of a second, and secondly in terms of computer life and transistors at the scale of nanoseconds. Virtual objects are avatars, pseudo-living entities, with a personality and sometimes a personality and an ethics, to assist people or to dictate the action to be taken in a certain context. Empowerment comes into a shifting process, not empowering to virtual subjects, like Frankenstein, but to those who design and manage these virtual computing entities. Technology competition takes a new turn: the most powerful governments delegate their secret to high-tech companies to push their ideological, political and economic pawns, colonize the people with digital culture and stifle the nations that do not have been able to undertake ambitious digital industrial policy.

While Europe works hard on regulation of personal data, "border line" service providers rejoice, because nothing will change on the essentials, namely software, source of authentic sound or malicious computing action.

ICT interconnects massive public communities (concentration of Big Data)

The proliferation of new technologies such as online social networks, cloud computing and Internet of Things, calls for innovative ideas to fuse, analyse, retrieve, filter, integrate and display data from a large number of diverse data sources. Big data is an emerging paradigm applied to datasets whose size (volume/velocity/variability) is beyond the ability of commonly used software tools to capture, manage, and process the data within a tolerable period of time. Such datasets are often from various sources yet unstructured such as social media, sensors, scientific applications, surveillance, video and image archives, Internet texts and documents, Internet search indexing, medical records, business transactions and web logs; and are of large size with fast data in/out. More importantly, Big data has to be of Big (high) value, and should be protected in an efficient way. Since Big Data involves a huge amount of data that is of high-dimensionality and inter-linkage, existing trust, security, and privacy measures for traditional databases and infrastructures cannot satisfy its requirements.

Future threats and vulnerabilities at the international scale

Threats in the digital world

We are always surprised that it is as easy to steal data, profiles of people can be used for commercial purposes, that identity of persons can be spoofed easily. Why researchers and software providers do not invent tools to prevent these fraudulent actions, why do we let these white collar bandits exist? The traditional answer is we want to preserve as much as possible anonymity on the network, so that everyone is used to or misuse. Software publishers do not want people file on the network by strong authentication and thus detect in real time who is doing what. We do not even try to offer solutions to those who agree to be on file with their consent, in exchange for peace found (with identification-authentication protocol with non-repudiation protocols at sending and at reception). The answer is also we do not want to question software copyright issues. Software publishers accept no responsibility: a computer program is a work of art. Only the end-user, who has generally no computer knowledge, is responsible for her actions after clicking the contractual acceptance

(usually incomprehensible) to use the service. This finding of user's submission face to software providers' omnipotence is a concern.

The dissymmetry of software and data within the ecosystem

The Internet ecosystem is characterized by the emergence of two complementary poles which clash: the data pole with data belonging to individuals and businesses, and the software cluster with services belonging to ISPs. Internet is both data and automated abstract machines (equipment and software). Service providers collect user data, record information about customers or subscribers, and are trading their profiles, in the absence of technical and legal means to stop them; the volume of personal data is measuring their financial ability by their potential of capturing information about users. Much citizens react by putting pressure for better control. Governments and intelligence services monitor infrastructures and use the legal arsenal by diverting it according to their own interests. Citizens react by putting pressure for greater transparency in governance. Moreover, the internet giants have verified the significant drop of turnover since the revelations of Snowden. Whistleblowers, from all countries, are likely to increase in the years that will come.

A clonable world

The digital logical world (software and data) is different from the physical world: it is a clonable world: there is neither original nor copies. After creating a first version, there are only clones that can be multiplied, but also be falsified, plagiarized or destroyed. It is difficult to manage the intellectual property of digital entities, because anybody can copy an original, modify it, and declare that the new clone is actually the real first version. It is also a world where anyone advances masked by the intermediation of a digital interface, so it is difficult to discern the authenticity and truth. It is a world where transparency does not exist, because it is difficult to prove a fact or event. Everything is a matter of trust: we must constantly assume that the person at the end of the line is who she claims to be, and we must wager it is in all kindness. These assumptions were confirmed at the beginning of the computer age, but this is no longer the case. When using computers nowadays, we fear constantly whether we are traced, profiled, spied by an attacker, a potential competitor, a supplier on the network, or by government services. In transactions on the network, it is not certain that an intruder is not going to steal our identity, enter our bank details or disclose our personal information. Court is of little help, because international law is in its infancy, and justice is slow and expensive. It is not sure that digital laws of our country and our continent are able to protect effectively.

Flexibility is the main threat

The digital world has open, wide and flexible specifications. This freedom is necessary to streamline its usage, and avoid rigid relationship in human-machine interfaces. Without even divert the normal use of the internet, it is possible to act maliciously, using naturally the applications. This permissiveness, coupled with anonymity and trans-boundary connections, breaches to all kinds of attacks such as denial of service by flooding the network resources or computing servers. In the near future, failures or attacks, which will affect both computers and the related physical mechanisms (manufacturing industry, transport, health) or inhibit

activity into enterprises (breakdowns for real-time applications, dysfunction in the electronic commerce), might be dramatic.

Overall weaknesses in the use of the ecosystem

Threats to this ecosystem come from the great flexibility in the use of these systems: failures, attacks, errors of usage, design, manufacturing or often operating, wrong update software version, system misconfiguration, lack of information of operating parameters, ignorance of the consequences of personal information publication, media lynching...

Yore, attackers were only computer experts, who exploited vulnerabilities of systems. These attacks still exist (zero day attacks), they are exploitations of unknown, undisclosed vulnerabilities. Nowadays, software attacks are downloadable and anyone can improvise striker, cryptographer, cryptanalyst and password cracker. Large-scale failures exist more and more. Breaches of privacy are more difficult to detect or to sue. Multiple, often free, standalone software applications are downloadable on the network. Anyone ignores what they hide of privacy invasion: storing diaries, smartphone geo-location, etc. There are also great cultural differences: European citizens want to keep secret of their personal data (legacy of totalitarian or authoritarian European governments during the twentieth century), the Anglo-Saxon see it as a way to negotiate and enjoy benefits, exchange against a service.

Regarding security, the main idea in this evolving ecosystem, into permanent extension is the notion of digital identity. A digital identity is a computer subject that is performing to a given time on a given space on computer machines (usually specific software that runs on universal physical machines), using data collected and previously digitized. The digital identity is driven by a natural or legal person responsible. But nowadays, it is possible to dilute this close relationship into the relationship between the real world and the digital world, with architectures peer-to-peer or with virtualization capabilities. In these scenarios, the notions of data processor and data controller are difficult to define.

Secondary issue in this ecosystem is the notion of accountability: who is at the other end of the line of my connection, who is answering to me? In general, the entity is anonymous and traceable through an address: an address of a Web site, a connected device by which responses are received. This subject may be benign (reliable search engine, call centre or trusted website, physical person who answers honestly, electronic commerce server, forum of authentic discussions). But the responding subject to the end of the line, can be malicious in varying degrees. It can monitor transactions for statistics, collect personal data to categorize individuals in communities, in order to trade in personal data without the consent of clients. It can hide its true identity for criminal reasons. Anonymity on the network is the main threat source.

Uncertainties about architecture of the global infrastructure

The revelations of E. Snowden have caused an earthquake in Europe, with the population, slightly less with political leaders. People have finally had tangible evidence that they were spied, and their rulers. Only BRICS leaders protested against this great espionage, as was witnessed at the recent Observer Research Foundation (ORF)[2] /

[2] http://orfonline.org/cms/sites/orfonline/home.html

Federation of India Chambers of Commerce and Industry (FICCI)[3] Cy Fy 2013, the "India Conference on Cyber Security and Cyber Governance" held in October, 2013 in New Delhi,, to which the BIC project coordinator and International Advisory Group (IAG) India members actively participated [3]. On this background, the BRICS nations have agreed on the establishment of an expert working group on cyber-security that will meet in early 2014, in South Africa [4] and similar efforts are underway between India and the US [4]. Conversely, European leaders are divided and remained silent. The revelations have especially emphasized the weakness of Europe in the digital domain, since European policies, initiated in the 2000s, failed.

The stability of the international infrastructure is raised. Emerging countries question ecosystem consistency (compatibility, interoperability or only interconnection) and international access. Walls on the border of continents may be erected in front of digital infrastructures if the Western world, particularly the United States, continues to want to assert their influence, spying widely the different countries, under the guise of the fight against terrorism.

[33] http://www.ficci.com/

2.3 Report structure

This BIC recommendations report provides an analysis of inputs received for the project's international platform building carried out in WP2/WP4. It also includes the inputs from the Working Groups established by the project, its foreign visitations, workshops, and other activities and initiatives where BIC participated in and contributed to.

This deliverable is organised in the following sections:

Section 3 is entitled Foreseeable bi-lateral co-operations between the EU and BIC countries and examines the possibilities in terms of potential, or already occurring, bi-lateral activities between the EU and the BIC Countries of Brazil, South Africa and India.

Section 4, entitled Recommendations for International Cooperation, lists the Strategic and Tactical recom-mendations and describes the rationale of the new threats and vulnerabilities of the digital ecosystem due to the evolution of technology and usages.

Section 5, entitled Priority topics and roadmap for international cooperation in security research, describes and analyses the main priority topics of research for international cooperation, provides a proposed timeline for the recommenadations, examines the priorities in ICT security research from the BIC Countries Brazil, South Africa and India.

Section 6, entitled Conclusions summarizes the deliverable report.

Section 7, contains the references and links for the report.

Annex 1 contains the in – depth prioritisation of research topics for each of the individual BIC countries.

Annex 2 contains an analysis and mapping exercise carried out looking at the priority research perspectives of Brazil, India, South Africa and the EU.

Annex 3 contains a summary and analysis of the recommended actions for H2020, for the implementation of international cooperation and trustworthy ICT originally contained within D3.1 - Interim recommendations report on future global research challenges in ICT trust and security.

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

This section examines the possibilities in terms of potential, or already occurring, bi-lateral activities between the EU and the BIC Countries of Brazil, South Africa and India. This section also begins with a summary of the EU approaches to trust and security research for the readers from outside Europe. Additional details on where the EU-International research challenges for each of the BIC countries can be found in Annex 1, which contains the background, research challenges and derived research priority details summarised individually for each of the BIC countries. A mapping exercise was also carried out between the countries approaches to Trust and Security research themes and this can be found in Annex 2, which forms the basis for the analysis in this report.

3.1 Europe

Background

Europe recognises that it needs an effective digital global strategy and Research and Technological Development (RTD) 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 heart-breaking 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 DG CONNECT (Communications Networks, Content and Technology), through its "Trust and Security" unit H.4 [5], 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.

The "Trust and Security" unit H.4 falls within the portfolio of the DG-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.

Furthermore, DG-CONNECT 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 multi-disciplinary research and the relevance of aspects like usability, societal acceptance and economic and legal viability of the research results.

Through DG-CONNECT Unit H.4, 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.

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

- Elaborate a European strategy on Internet security and remove cybersecurity 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

An H2020 information day is being held by the DG-CONNECT Trust & Security (H.4) unit on 15th January, 2014 in Brussels.

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.

3.2 Brazil

Background of Research funding agencies

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

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.

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:

The first BR-EU coordinated call (FP7-ICT-2010-EU-Brazil) [6]

Preparation work for this call started in September 2009, in which there were two international workshops held in Brazil examining EU-Brazil cooperation on new architectures for the FI. Members of the BIC project, including IAG members were actively involved in both the EU and Brazil delegtations. As a result of this efforts, in September 2010, the CNPq (National Research Council) of Brazil and DG INFSO (predecessor of DG CONNECT) 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, due to the budget level available.

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).

The second BR-EU coordinated call (FP7-ICT-2013-EU-Brazil)

The second ICT – EU Brazil Coordinated Call was part of FP7-ICT-2013-EU-Brazil [7], with a budget of 5M from each country. There was no specific call area addressing Security, but instead had the following areas of coverage:

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.

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

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. Some 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.

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-ICT-2010-EU-Brazil between the EU and Brazil including one topic on Future Internet - Security.
- A coordinated call was already held in EU FP7-ICT-2013-EU-Brazil between the EU and Brazil, which didn't specifically include trust and security topics.

One of the goals of the BIC project, especially with the newly lauched BIC Extended Working Group [8] 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.

We are happy to report there is already a new joint call within the Horizon 2020 programme within **H2020 – EUB – 2015** [9] between the EU and Brazil with an increased budget of 7M on each side in the following topics:

EUB 1 – 2015: Cloud Computing, including security aspects - Specific Challenge: Data are motivating a profound transformation in the culture and conduct of scientific research in every field of science and engineering. Advancements in this area are required in terms of cloud-centric applications for big data, as well as in creating novel cloud technologies that provide effective utilization and optimization of heterogeneous resources (such as storage and communications) in big data scenarios, in particular addressing privacy, security and other Quality-of-Service issues. (Budget of 3.5M euros)

EUB 2 – 2015: High Performance Computing (HPC) - Specific Challenge: The work aims at the development of state-of-the-art High Performance Computing (HPC) environment that

efficiently exploits the HPC resources in both the EU and Brazil and advances the work on HPC applications in domains of common interest. (Budget of 2M euros)

EUB 3 – 2015: Experimental Platforms - Specific Challenge: The objective of cooperation in the area of Experimental Platforms is to enable and promote the federation of experimental resources irrespective of their localization in Brazil and in Europe, with a view towards global experimentation across heterogeneous networks, both wired and wireless, and a variety of end-systems. (Budget of 1.5M euros)

Although details have emerged for this call in the first call text of H2020, the final H2020 – EUB – 2015 call will be published in December 2014 and will have an expected deadline on 21st April, 2015 with a total budget of 7M Euros expected from each side as broken down above.

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.

- **International cooperation in Cybersecurity:** 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.
- **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 and Security:** 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.

3.3 South Africa

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

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) – http://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.

Key research focus areas for collaboration

International cybersecurity 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 cybersecurity 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 cybersecurity alliances (universities, industries, banks) that share information / best practice.
- Opening up international data-exchange architectures for cybersecurity.
- Models and platforms for national and regional cybersecurity coordination (citizens, industry, security sector, government, regional governments).

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.

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 on-going 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.

SOUTH AFRICA - EU collaboration 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:

- The BIC project has actively contributed to all of the EuroAfrica-ICT Cooperation Forums during 2011 [10], 2012 [11], and 2013 [12]. During the 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 CONNECT 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 [13] and added further value and clarity to joint EU/Africa research priorities in Trustworthy ICT. Similarly, during the 6th EuroAfrica-ICT Cooperation Forum on ICT Research, 4-5th December, 2013, Addis Ababa, Ethiopia, the BIC project co-organised a session on building international cooperation 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.
- It was agreed at the BIC Annual Forum during 2012 that the BIC Working groups would include members from beyond South Africa in the wider communities in other African countries. This has already happened with the establishment of the BIC Africa Extended Working Group (EWG) including members from Africa [14].

3.4 India

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 RTD, 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.

Key research focus areas

During the BIC organised workshop in December 2011 [15] 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 Department of Electronics and Information Technology (DeitY), Govt. of India Cybersecurity R&D Group[4] when they met with BIC in December 2011, and later during the interactions in setting up and running the BIC India Extended Working Group [16]. The DeitY Cybersecurity R&D Group is the closest peer to the Trust and security unit in the European Commission, which lays emphasis across the Trust and Security spectrum - Basic research, Technology demonstration and Proof-of concept and

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

R&D test bed projects. It stems from the consideration that indigenous RTD 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.

Research Thrust areas in cybersecurity R&D department of DeitY

The areas of near to medium term public-funded Information Security research in India under the aegis of the cybersecurity R&D department within the Department of Electronics and Information Technology (DeitY) 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[5], who are a member of the BIC India EWG, advocating strong privacy and data protection as a lever for economic

[5] http://www.dsci.in/

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."

- 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 cybersecurity 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.

Conclusions

Following the mapping exercises and analysis carried out by the project for India (see section A1.2 in 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: International Cooperation on Cybersecurity

The first theme is international cooperation specifically on the topic of cybersecurity as it is a global issue, requesting a global approach to alleviate the increasing ICT-related risks. To be successful, international cooperation to promote cybersecurity must be built on sound national organizational structures. National strategies to promote cybersecurity 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 cybersecurity 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 cybersecurity. These efforts could lay foundations for a framework for international cooperation in cybersecurity.

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, cybersecurity research must encompass a large range of ICT disciplines: technological (data, software, network, cryptology, etc.) and societal (economy, ethics, sociology, criminology, etc.).

Strong 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. Another meeting is expected in 2014 and BIC can make a contribution, if required.

Theme 2: 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 3: Trust & Privacy

This third 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 4: Global Frameworks for multi-lateral cooperation and international alignment

The fourth theme of cooperation is concerned by the need for moving beyond the tactical bi-lateral cooperation model and moving towards a more strategic multi-lateral model of cooperation. The India representatives on the BIC IAG and WG3 have spearheaded this theme and have suggested and reworked a very successful extended structure to the BIC collaboration platform to include in-country Extended Working Groups to be established in addition to the BIC Core working groups. This structure has now been set up in all three BIC countries and will continue after the conclusion of the BIC project. We won’t go into detail here on this long term strategic model as spearheaded by the India members because this extension to the BIC structural components is explicitly detailed in WP2 deliverable D2.5 - Final Report of the Working Groups Activities.

Theme 5: Engineering and Scientific domains

The fifth 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 disciplines. These include:

- 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 the loss of a customer's confidence on the businesses; or make them liable to penalties if some business critical security breach information is not shared with the stakeholders.
- 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 cybersecurity 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.
- 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?
- 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 work out their effectiveness in the contemporary distributed systems.

4 - Recommendations for international cooperation in Trustworthy ICT

This section details two groups of BIC recommendations, a strategic group and a tactical group, with their specific rationales for inclusion detailed accordingly. The two recommendation groupings, as shown in Figure 3, are not meant to be consecutive, but to address two parallel aspects of the field of necessary international RTD. The groupings are defined as follows:

- ***Strategic Recommendations (SR)***: setting out the frameworks, common understandings, and overall procedural and governance landscape that takes into account the diversity of social, economic, and cultural norms and requirements worldwide. These can be considered as ground rules and enabling actions that must take place to facilitate effective outcomes of international cooperation in this field in order to carry out the specific (tactical) recommendations.
- ***Tactical Recommendations (TR)***: more specific or concrete research recommendations to progress towards the required technical building blocks and their relationships that will enable a trustworthy ICT ecosystem. Trustworthy ICT is defined as ICT that is secure, reliable and resilient to attacks and operational failures; guarantees quality of service; protects user data; ensures privacy and provides usable and trusted tools to support the user in his security management. It is expected that the newly formed EWGs, in conjunction with their supporting governments and also continued interaction with the EU Commission delegation will also continue to add to the tactical recommendations in the near future as they continue their work.

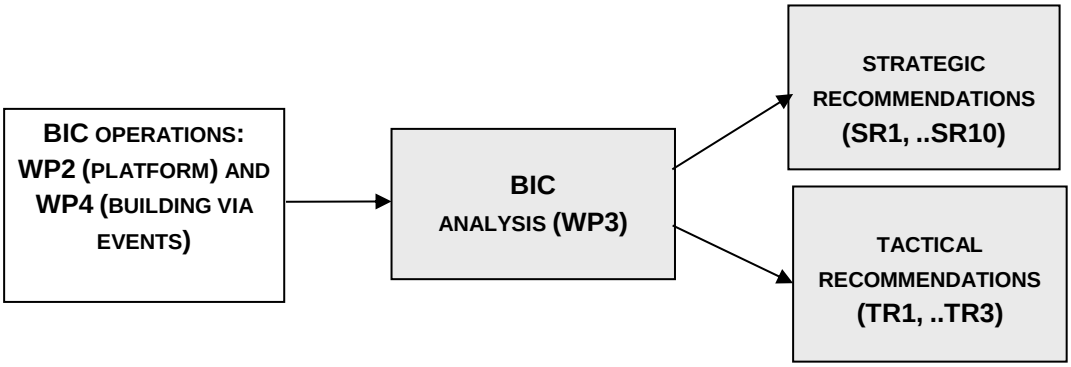

Figure 3. BIC recommendations structure

4.1 The changing landscape of security research

SR1 Need for new global approaches, meta-models and methodologies

Rationale SR1.1 There is a risk of fragmentation of the ecosystem and we need to consider new holistic global meta-models taking into account diversity

With the continued computerization of society, the emergence of Internet of Things will undermine the notions of identity, privacy and intellectual property. These concepts must be rebuilt in the digital world on a new basis, since digital world is by definition a world where clones are consubstantial, where forgetfulness and trust do not exist, and where notions of space and boundaries are blurred with virtualization. Vulnerabilities will be multiplied in the intertwining relationships between objects and the traces left by these objects. To prevent these abuses, we must abandon the pre-written marketing idyllic visions and rethink on new models, counter-models and alter-models of communication network. The E. Snowden's revelations are moving lines of internet governance in BRICS countries, which would aim to get rid of a unipolar internet. As mentioned earlier, this was a hot topic at the recent Observer Research Foundation (ORF)[6] / Federation of India Chambers of Commerce and Industry (FICCI)[7] Cy Fy 2013, the "India Conference on Cyber Security and Cyber Governance" held in October, 2013 in New Delhi, to which the BIC project coordinator and International Advisory Group (IAG) India members actively participated [3]. On this background, the BRICS nations have agreed on the establishment of an expert working group on cyber-security that will meet in early 2014, in South Africa [4] and similar efforts are underway between India and the US [4]. Europe must also get on board with these discussions. Fragmented sky with satellite constellations (GPS in United States, Galileo in Europe, Glonass in Russia, Beidou in China, IRNSS in India) is showing the way of a continental sovereignty that will touch down sooner or later on the Earth, on the fiber optical submarine cables and network access providers' infrastructure. Diversity, essential property of life on the planet, should apply in all areas of human activity.

Rationale SR1.2 Some fundamental concepts are not yet fully expressed in computer science terms and are not instantiating cultural features

However, in general, technical aspects are relegated behind the usage topics. For example, research in cryptography seems less imperative than the development of technical and legal mechanisms to respect for privacy. Discourses on respect of privacy, on abuse of personal data, on recording and processing navigation and communication metadata without the consent of individuals have gained considerable importance on security research roadmaps. However practical applications and implementations are still sorely lacking nowadays. Similarly, models of trust and reputation exist without real operational services. The instrumentation of still too general concepts cannot be possible in computer science. We must refine the variables involved for trust and privacy, depending on culture and depending on context, to contain further specifications.

[6] http://orfonline.org/cms/sites/orfonline/home.html
[77] http://www.ficci.com/

Rationale SR1.3 There is a need for quantitative security assurance and trust in architecture design, software engineering and international recognition (transparency)

There is an increasing demand for techniques to deal with quantitative aspects of security assurance at several levels of the development life-cycle of systems & services, e.g., from requirements elicitation to run-time operation and maintenance. It remains a challenge to design, analyse, evaluate, and improve the reliability and security for a trusted computing environment. Trusted computing targets computing and communication systems as well as services that are autonomous, dependable, secure, privacy protectable, predictable, traceable, controllable, assessable and sustainable. The scale and complexity of information systems evolve towards overwhelming the capability of system administrators, programmers, and designers. As a promising means to implement dependable and secure systems in a self-managing manner, autonomic computing technology needs to be further explored. On the other hand, any autonomic system must be trustworthy to avoid the risk of losing control and retain confidence that the system will not fail. Trusted and autonomic computing and communications need synergistic research efforts covering many disciplines, ranging from computer science and engineering, to the natural sciences to the social sciences. It requires scientific and technological advances in a wide variety of fields, as well as new software, system architectures, and communication systems that support the effective and coherent integration of the constituent technologies.

Rationale SR1.4 Outsourced data storage and large scale virtualization remain a major security challenge

Communication security, strictly speaking, has reached a satisfactory level of reliability and poses fewer problems. However data storage remains a major challenge, as these data repositories are operated by opaque applications without the consent of owners. As for security of computations, it is a matter of fundamental research, with a little attention so far. Research focuses on correct software, but very little about their dangerousness or fragility, as these concepts are difficult to describe in computer science. Thus, the essential vulnerability of the ecosystem remains the lack of technical means (access and control) to ensure the data protection under the control of software driven by others, without the knowledge of owners. With virtualization of communications, storage and computations, the location of the ICT operations control has become opaque, so that service providers can use this new mechanism to their advantage, especially when courts require locating versus time and space, malicious acts, which is now impractical. The mission of absorbing these new ICT concepts by legislation is a task of great urgency, and that's only internationally that these issues can be addressed.

Rationale SR1.5 Massive global networked phenomena bring another order of magnitude in protection complexity

International research must understand new situations such as cross-border ICT operations, security of individual transactions in real time (mobile security, protection of children, and payment through mobile terminal), and security in a virtual world. It must also differently understand volatility of commands, speed of operations and massiveness of ICT phenomena. Anomaly detection is a very different exercise depending on the volume of the

search space. The too rigid and too simplistic security policies (by perimeter or in depth), were shattered in recent years, with the advent of widespread use of wireless communications, within company and outside company, cloud computing for personal and business applications, and new usage in business as BYOD (“bring your own device”) which combines responsibilities of the digital identity from the person and the employee. Actors’ responsibility is indented, as it is diluted in new concepts and massiveness. Research focuses now on the concept of accountability to deal with these operations, this concept being most striking for evidence but less interesting to highlight operator's or service provider's responsibility. The search for weak signals in large areas (network traffic analysis, Big Data security, safe calculations) becomes a matter of vital research to manage the ecosystem.

Rationale SR1.6 The future Internet of Things, a birth of digital intermediation without governance, requires new security architectures, new global object identifications and new security models

Slowly, a computer interface was formed as a sort of thin lens between humans and reality. Physical and logical organizations are managed by ICT. We can only perceive or understand reality through the distorting prism of ICT. We observe (or sometimes produce) social reality by the intermediation of ICT instruments. This digital interface is a source of empowerment, opportunity, innovation, knowledge. It also has become over time a wasteland, a corridor of violence, which intersect cyber criminals who defraud, service and content providers who are innovators of the "border line" applications, and governments that use or misuse with their power. These three categories have rushed into this crack without governance to operate modernity without the users’ knowledge. Impersonating, phishing, unintentionally soliciting, spying, monitoring, misinforming... become the current operations of these illegal and legal organizations, against which each of us must guard every moment, in an unequal face to face on her smartphone or her computer. This corridor should have been a quarantine zone, a DMZ, where everyone could have negotiated, legally and transparently, her behaviour and her relationship with others according to contextual rules of governance. Mercantilism and the cruel rules of technology evolution have taken over humanism, and have put legislation, regulations and regulatory authorities with a fait accompli.

The Internet of Things was born from RFIds emergence and IPv6 capacity to extend identity cardinal potential. These myriads of sub-networks of mobile objects, built around the internet, could be despotic or anarchic. Soon, citizens, consumers, patients in the various facets of their roles, will be living in an intensive digital medium. They will live in homes connected to smart grids to better use energy. These buildings will be located in smart cities, where camera networks will mesh city space, with digital displays on streets, digital aids for parking or transportation. These cities will be equipped with sensor networks, populated by robots. Drones will circulate to accompany official and festive events. Complex, dynamic, scalable, pervasive massive ICT will be hardly mastered, and will generate mosaics of vulnerable microcosms.

The Internet of things moved to the outskirts of this highly computerized internet. It has itself evolved. While it was directed in 1998 to a reading and connecting to a radio tag attached to a manufactured article, with a traceability function, the Internet of things has become an internet connected objects, be it cars, robots, sunglasses and watches, electronic

valuables, connectable to the network and controlled remotely via a smartphone. The outskirts of this ecosystem will be split to reveal an architecture with scales and gateways that will protect these sub-networks with objects. These protection gateways, in front of subsets of connected objects, will be interconnected similarly to existing triple-play (telephone, internet, television) boxes for connecting our homes.

Internet of Things will include not only logistics objects with RFIds but other smart things: cars interconnected to manufacturer network, swarms of interconnected objects connected to home owners, medical devices of hospital connected to health sensors for ambulatory medicine, etc. Interconnection will drive traceability and lifecycle of manufactured object. It will be also living beings: people with Alzheimer's, also plants or pets. In addition, satellite constellations will allow geo-location of all these nomadic entities. The advantage of internet of things lies in the fact that objects may communicate with each other without human intervention. In a more distant future, invisible objects, "smart dust", especially for health, would also be interconnected via electromagnetic or mechanical forces. Massiveness (100 billion objects connected?), fragmentation of digital interfaces, proliferation of digital connections, rise of insecure applications' rains on smartphones, fragmentation of new threats (cyberactivists, haktivists, cybercriminals, pressure groups, criminal groups), will sweep out traditional security technical measures. It will then be necessary to reconsider canonical computing architectures. For example, to formalize threats into a mobile world, it may be more profitable to use enthalpy models, where the momentum (the activity heat) occurs rather than referring to C. Shannon's information theory, which takes into account entropy. To protect smartphones and personal computers, it should probably be necessary to not work in solo, each with her own personal shield (antivirus and firewall functions independently of the others), which makes the fortune of security software manufacturers today. Instead, we will require solidarity and cooperative protection models.

SR2 Cybersecurity is a moving landscape of attacks, surveillance and failures at the global scale

Rationale SR2.1 Threats are more and more related to borderless massive usage of the network, with crowd effects

It is difficult to define research priorities in security at the international level, both lines of research are interrelated and as evolving threats varies more by the development of usage than through technological innovation. But underlying trends are emerging in most countries. The changing and diverse nature of usage influences the emergence of different threats, and at the same time, the priorities of security research.

In 2013, in the business sector, irreversibility of data storage abroad, by outsourcing and cloud computing, is undermining industrial digital heritage. Similarly, exposure of personal data by individuals on social networks, and of multimedia files belonging to audio-visual authors, stored by hosts on the Web, is threatening extensive digital identity of individuals and intellectual property of multimedia content.

Rationale SR2.2 The enlarged spectrum of international attackers is expanding

The range of attackers has also expanded in recent years. The activist who is in the light, joined spy who is in secret, and fraudulent acts in anonymity or via identity theft. The target is not necessarily the computer object but often the image of this object. Gain money or knowledge of information, alteration of a system or destabilization of a population, are then supplemented by misinformation (media lynching, defamation, harassment, rumours). The main threat of internet is identity fraud. This threat is exacerbated by the fact that transactions are a priori anonymous on the internet.

Rationale SR2.3 The underlying cyber-war between cyber-tectonics plates is emerging

At the state level, there are two main threats: attacks between states, through agencies or parallel services on the one hand, and monitoring of activity, communications networks and servers, via agencies, service providers, or internet giants, on the other hand. If attacks between states are still in the shadows, they were nevertheless revealed last ten years by cases such as Estonia in 2007. The revelations made by the US' ex-Central Intelligence Agency employee, Edward Snowden, in various interviews to The Guardian newspaper, revealed that the US' intelligence organisation, National Security Agency (which had launched the top-secret PRISM programme) was snooping on personal data of individuals and governments in the US and across the world through the internet, particularly in Europe. He also revealed that the National Security Agency (NSA) intercepted sensitive information that belongs to India by spying on the embassies[8]. And the information sharing between the intelligence agencies of various countries, such as the US and the UK, is already underway. In this complex cyber-scenario, where the United States has the maximum advantage, with most of the internet traffic flowing through the US servers, it is premature to talk about cyber-war. Even though there is no common agreement between all the countries on matters of cybersecurity, some of the countries started working together.

Rationale SR2.4 The worldwide surveillance of networks, and people activity cannot be done in total darkness

For non-democratic countries, monitoring communications in their own country were a known fact (espionage, filtering and censorship). Following the revelations of Edward Snowden, digital surveillance in democratic countries, was revealed to the general public, as a practice that could be justified by the fight against terrorism. Moreover, monitoring of computer data across the globe, with the complicity of traditional service providers (Google, Facebook, Microsoft…) surprised the public by its size and its extension outside the U.S. States, to include the whole of Europe. It is difficult today to assess the impact of these operations on the edge of acceptability by citizens. If terrorism concerned citizens, they must be informed and their political representatives should be able to assess finality and proportionality of the means used to fight against terrorism.

[8] http://www.forceindia.net/DomainSafety.aspx

4.2 International cooperation framework

SR3 International cooperation in research should be an essential H2020 requirement

Rationale SR3.1 The fragile and interdependent construction of the digital ecosystem must be made more robust and secure, under international supervision

Cybersecurity is becoming one of the greatest issues for government, business and individuals. Attacks are initiated by individuals, private enterprises, secret services as well as countries. In this they include the government, company, organization networks or simple individuals, depending upon whether attackers are criminals, cyber-activists, cyber-haktivists or spy, whether attackers are violating users' identity for frauds, intimidating their target, pursuing industrial intelligence, or conducting diplomatic espionage.

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 country. 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 cybersecurity 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.

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, cybersecurity research must encompass a large range of ICT disciplines: technological (data, software, network, cryptology, etc.) and societal (economy, ethics, sociology, criminology, etc.).

Rationale SR3.2 There is a need to define and use international cooperation research based on existing structures for a resilient ecosystem

To be successful, international cooperation to promote cybersecurity must be built on sound national and continental organizational structures. National strategies to promote cybersecurity 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.

International research programmes with joint efforts between nations and continents 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 cybersecurity. These efforts could lay foundations for a framework for international cooperation in cybersecurity.

International action must include both security of network infrastructure and services, and maintaining trust of individuals, businesses and governments. The ecosystem must be resilient against large-scale failures or attacks, or targeted failures and attacks on a region, a company or a community, regardless of frontiers. Measurements should prevent attempts and avoid to weaken or to destabilize this interconnected world.

A U.N. study, of February 2013, titled "Comprehensive Study on Cyber Crime" [17] is addressing the legal framework in order to put sufficient, international regulation in place, with the following key results: the technological developments associated with cybercrime mean that - while traditional laws can be applied to some extent - legislation must also grapple with new concepts and objects, such as intangible 'computer data,' not traditionally addressed by law. Legal measures are crucial to the prevention and combating of cybercrime, and are required in all areas, covering criminalization, procedural powers, jurisdiction, international cooperation, and Internet service provider responsibility and liability. At the national level, cybercrime laws most often concern criminalization - establishing specialized offences for core cybercrime acts. Countries increasingly recognize the need, however, for legislation in other areas. Compared to existing laws, new or planned cybercrime laws more frequently address investigative measures, jurisdiction, electronic evidence, and international cooperation. At the last World Economic Forum in Davos, Switzerland, cybersecurity was a topic of discussion among top world CEOs. Strong economic interests by large Internet firms will prevent or significantly slow down the movement for global web regulation.

Rationale SR3.3 Although there are strong restraints and difficulties of international cooperation at the state levels

There is no common international understanding of the term "cybersecurity"[9] which seems insufficiently clear to the general public and to experts. Cybersecurity (cybercrime and cyber terrorism) are a matter for diplomacy, policy, economy, ideology and technology. The European Network and Information Security Agency (ENISA) says that at both the intra-European and international level, a harmonized definition of cybersecurity is clearly lacking. National approaches to cybersecurity strategies differ and the lack of common understanding may hamper international cooperation [18]. An European "Internet Security Strategy" must be developed to propose governance frameworks and set goals for incident response. The

[9] The Center for Strategic and International Studies (CSIS) defines cyber terrorism as, "The use of computer network tools to shut down critical national infrastructures (e.g., energy, transportation, government operations) or to coerce or intimidate a government or civilian population." The US Federal Bureau of Investigation (FBI) generally sums up cybercrime as the following offenses: computer and network intrusions such as bots, worms, viruses, spyware, malware, hacking and identity theft. The International Telecommunication Union defines cybersecurity as a "Collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance, and technologies that can be used to protect the cyber environment, including organizations' and users' assets."

USA is setting up a cybersecurity hotline with Russia analogous to the "red phone" Cold War system. Substantive joint U.S. and Chinese efforts for international cooperation are uncertain.

Rationale SR3.4 An agreement for cybersecurity strategy is needed for citizens' usage at the global scale

Telecommunication companies, internet service providers (ISPs), and other private sector actors now actively manage, monitor and control networks. Pressures to regulate the global network of information and communications have never been greater. States were once thought to be powerless in the face of the global communication surveillance. The future of the whole ecosystem will be determined by the various ways governments will react to these problems. The future relationship between citizens and communication infrastructures will be modified by the overall decisions. The global governance will influence all the new security architectures: cryptography algorithms and standard in cryptography, key and certificate management, identity management, authentication protocols (biometry, etc.) and interoperability in security functions.

The greatest challenge of security research in the next ten years is this agreement on a comprehensive security strategy for the digital ecosystem. ICT threats are now global exploiting the borderless feature of the cyberspace and the national aspects of justice. If this strategy does not come up to an international agreement, a balkanization of the ecosystem could arise at the region scale with separate continental plates: North America, Central and South America, Europe, Africa, Arab countries, China, India, East Asia, etc.

SR4 The international community must agree on grand principles of human values

The security enforcement follows human value principles that must be met: individual freedom, human dignity, individual privacy, intellectual property rights and free movement of ideas, people and assets. The transposition of these principles from physical space to digital space is not obvious.

Rationale SR4.1 there is a need to take into account ethical, legal and technological dimensions of trustworthiness of the ecosystem

The world must agree on the terms of cybercrime and cyber terrorism, and should combine efforts to address those issues that affect the whole. Measures are both technological and political. The technology component includes harmonization at the level of identity management, authentication procedures, certification procedures, management of evidence, recording logs, protection of privacy, accountability. Policy measures are constitutional, legislative, legal, regulatory, organizational arrangements to harmonize internationally, methods and tools.

Rationale SR4.2 Accountability versus responsibility of service providers must be viewed at the global scale to take into account the general interest of all citizens

In cyberspace, the relationship between the attributes of a digital identity and the responsible person is difficult to establish. That is the question of the difference between accountability of digital actions and behaviour across networks on the one hand, and individual responsibility acting with intent, here and now, freely and knowingly on the other hand. You can be countable of a digital action (launching a virus attack or a botnet) from your computer without being legitimately responsible, if the malware is hosted into the computer unbeknownst to the user, due to a failure of the operating system or a security breach of a poorly protected application.

Software vendors generally disclaim any responsibility with long and unreadable license contracts. The notion of software author's responsibility has virtually disappeared because of copyright: software is a work of art. International discussions are much more on the protection of personal information and not personal software, they almost do not cover the rules on software authors' and distributors' responsibility, software that capture and process personal data. Software publishers are hiding behind the concept of accountability, which tends to remove a maximum of responsibility to the service provider.

At the international level, it is essential that all actors feel responsible and do not come off quickly their responsibility, with illegible or asymmetric unfair contracts. The society that we are trying to build depends on us. It is important to think of the hopes and fears of the future that we will produce, and the technological and legal means to set up at the international research in digital security.

Rationale SR4.3 Diversity of cultures and norms for privacy and responsibility must be integrated and instantiated into the security models

The key notions of private life, personal data, accountability, responsibility, are not universal and an international digital right does not exist. It is therefore necessary to cooperate to closer views, harmonize or converge to stable solutions, or create gateways between the different approaches that avoid fragmentation of the whole. The concept of personal data (specific to identify a person, not necessarily the owner or the author but the person embodying the attributes, such as the footsteps - spatiotemporal coordinates – of the person's movement or traces of its circulation into the ecosystem) varies according to continents: the IP address is personal data in some countries but not in others.

We need to have a multipolar approach depending upon culture, history and level of digital usage: not a homogeneous, monolithic approach, but a framework taking into account diversity. Emphasis on responsibility of stakeholders, more than accountability is a new deal between "personal data" and "software which are processing personal data". Legislation must also be revised and more careful if we want to keep in Europe a good idea of democratic principles' enforcement.

SR5 In H2020 and beyond, for topics like cybersecurity, there must be a shift in emphasis from the tactical bi-lateral (country to country or region to region) collaborations to a strategic multi-lateral (strategic, multiple country to country or multiple region to region) approach for INCO.

Rationale SR5.1 Cybersecurity research requires a comprehensive spread of global participation.

One of the main objectives of the BIC project was to discuss how to move from a more tactical based approach (bi-lateral) towards a more strategic approach (multi-lateral approach) as seen in figures 4 and 5.

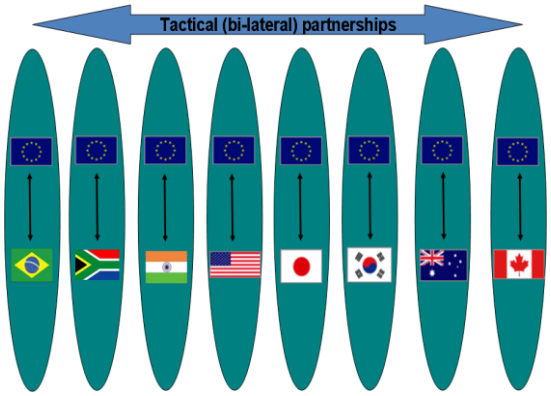

Figure 4. Tactical (bi-lateral) approach

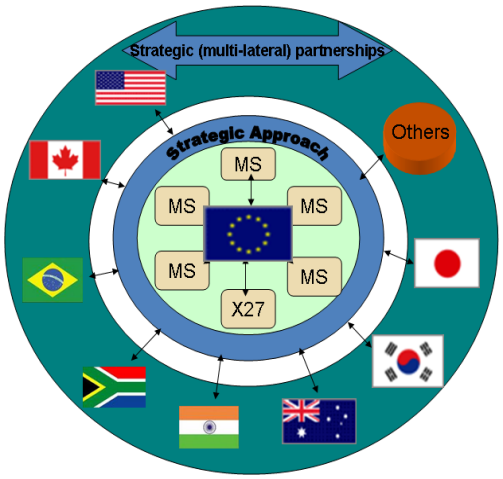

Figure 5. Strategic (multi-lateral) approach

Through their working group 3 (programme management / funding focus), the project made sure to include members from other international cooperation projects engaged in international cooperation with long standing expertise in both bi-lateral and multi-lateral international cooperation (working with governments and/or specific agencies) to enable the following outcomes:

1. discuss their experiences and insights in order to brainstorm a strategy to move forward on international cooperation in future calls for collaborative research;
2. Forming the current bi-lateral (and potentially overlapping) country to country cooperation into a comprehensive and coordinated global cooperation.

In addition to BIC, a wealth of experiences was represented from the following international cooperation projects: IST Africa, EuroAfrica-P8, FEED, AUS-ACCESS4EU, PACE-Net, EU – India Spirit, Synchroniser, Euro-IndiaGrid2, OpenChina-ICT, FIRST, FORESTA, PAERIP, SEACOOP, EuroAfrica-P8, IST-EC2 (EU funded FP6 project to foster research in ICT between Europe & Canada), and AMERICAS.

These projects gave their insights on their experiences and suggestions for improvement and the main point was agreement that it is a very good idea to move towards a more multi-lateral strategic position. However, in the discussions, it wasn't very clear how this strategy shift could occur within the current mechanisms that focus bi-laterally on a number of distinct regions. The BIC project has developed a cooperation platform that could be used, including the International Advisory Group, Core Working Groups and in- country Extended Working Groups that we feel is a good starting point towards moving towards the strategic multi-lateral approach. The recommendations regarding these will be covered in more detail in a number of Tactical Recommendations (TRs).

Rationale SR5.2 Bi-lateral INCO for cybersecurity leads to an asymmetric situation of the "weakest link".

While this regional approach may work for higher level themes e.g. ICT, the main difficulty arises when a particular research topic, for example, Cybersecurity, needs to be addressed globally and multi-laterally amongst many regions, the bi-lateral approach is not suited for this type of long term strategic activity. The main reason would be that one region may not consider a particular topic of research to be of same high priority as the other region. Or there may be a mismatch of the degree of appreciation or level of awareness and focus. Hence, on a topic of cybersecurity, each of the bilateral regions may indeed focus on something else in their respective bi-lateral activities leading to weak links in the chain. Therefore, if you have regions that are neither focussing, nor bringing together the right experts to participate in the same topic across the board with the other regions/countries, there will not be a consistency of equally strong focus on the topic of cybersecurity across all of the participating countries, leading to an asymmetry. This has already been proven in other bi-lateral activities, where the focus on some could be on smart cities, while others might focus on cybersecurity, and so on. The BIC approach was fundamentally different in which there is a uniform, consistency in the topical coverage across all of the regions being advocated from the start. Accordingly, there must be some inherent mechanism available to foster this desired of strategic cooperation across multiple countries/regions with consistency to deal with these important topics.

TR1 The work of the BIC project and mainly its structural components (IAG, WGs) should be functionally sustained from the long term perspective of at least 10 years, and also expanded to other countries, especially in terms of the cooperation platform components - International Advisory Group, Core Working Groups and in-country Extended Working Groups.

Rationale TR1.1 The INCO aspect of the BIC project has gained strong momentum whereas the core issue, the threat to Trustworthy ICT is still has a long way hence the momentum must be maintained for the project work and its multi-components.

The EU and BIC countries of India, Brazil and South Africa, should formally accept the necessity that the achievements by the BIC project thus far and its already established work are essential to continue in some functionalform, and there is need for continuity of a project like BIC and its main components for Trustworthy ICT for a longer time frame, extending for at least up to10 years or at least during the entire tenure of H2020, until such time that the in-country bodies like EWGs become stable and the multi-lateral cooperation through inter

EWG transactions becomes a self-sustainable and progressive reality. This is because of the nature of the underlying issue of sustained threat to Trustworthy ICT from “anywhere in the Globe”. It is, therefore, necessary for EU to consider it as “critically essential” to continue the efforts for sustained international cooperation on research and innovation in the area. Accordingly there should be a future coordination activity to keep these BIC components up and running. The roles of the individual and collective parts of the BIC structure are too important to let dissolve.

Rationale TR1.2 Continuity of the International Advisory Group (IAG) and Extended Working Groups (EWG) for Trustworthy ICT is critical for a bigger picture in view of the global landscape for the threat and corresponding research Requirements.

It is essential that the structures evolved under the project must continue to exist and function, especially the International Advisory Group and the Extended Working Groups (EWGs) must essentially carry on their work as per their role and objectives (as explained later, in detail). This is because while the tenure of the BIC project may be limited in duration to three years, its theme - “International Cooperation” for Trustworthy ICT is one of a permanent nature. It is, therefore, necessary to speculate the modalities to facilitate future functioning of IAG through regular interaction of its constituent members. Therefore, it is expected and desirable that the members of the IAG – the researchers, the industry and the government - continue to collaborate regularly within each country of BIC using now established country specific Extended Working Group (EWG), and they in turn find innovative ways to establish and continue collaboration with their peers in other countries as part of their stated terms of reference.

It would be essential that the European Commission and other Government programme management agencies of respective BIC member countries establish some possible options for continued functioning of the IAG, even if it needs to be in a scaled down version to a full project. Some options for this could be:

- Coordination or Support action under H2020;
- An ad-hoc and/or flexible funding mechanism should be set up specifically for the running of an IAG event bi-annually/annually in coordination with the associated bodies such as EWGs that have evolved under BIC. Note: there are already models for this kind of ad-hoc activity specifically for regular networking – a good example would be the United States’ National Science Foundation grants that have a fairly light weight mechanism for organising networking events, including travel and organisational costs. A number of these were presented at the BIC workshop during June 2013 by the NSF [19];
- A “sharing the burden” model, whereby one country of the IAG takes the lead role on a 6 month or 12 month basis for the IAG coordination, including the costs involved (in a similar way that the EU Presidency is organised and run where EU Member States holds the responsibility for periods of six months);
- Transfer the IAG activities to another running initiative/agency, or combination thereof of a number of initiatives/agencies, that would have funding available for its continuance and already holds an annual conference e.g. NIS Platform, CSP Forum, ENISA, Observer Research Foundation, Digital Enlightenment Forum, amongst others…

As for the BIC Core Working Groups, since they were mainly congregated to participate and contribute to the BIC Workshop events, as these events will not continue after the conclusion of the project in December, 2013, it is natural that the Core WGs will not continue as a formal body. However, a very positive development took place in the last six months of the BIC project with the establishment of the EU Network Information Security Public Private Platform (NIS Platform), which held a kick off meeting for their Working groups during September, 2013 [20] and a follow up plenary and WG3 meeting in December, 2013 [21]. The establishment of the NIS Platform is a key action of the EU cybersecurity Strategy and aligned with the implementation of the NIS Directive. The NIS Platform is developing a platform for trusted information sharing and the need for WGs with clear objectives and well-defined themes. Three working groups have been set up and their launch meetings were held on 25th, 26th and 27th September 2013, respectively:

- WG1 on risk management, including information assurance, risks metrics and awareness raising;
- WG2 on information exchange and incident coordination, including incident reporting and risks metrics for the purpose of information exchange;
- WG3 on Secure ICT research and innovation.

Subsequently, the majority of the BIC Core WGs members, including all the BIC partners, are actively (in some cases taking leading roles) involved in NIS Platform WGs, especially within WG3, where it will be possible to advocate the building of international cooperation for trustworthy ICT within these working groups.

The Extended Working Groups (EWGs) have been established to play one of the most crucial roles in building the in-country research collective body and effectively promoting the multi-lateral international cooperation. Hence, there is a strong need to continue and grow the EWG and the bodies set up under this concept in the participating countries viz. India, Brazil, South Africa (and wider Africa participation), and growing to other interested countries after the conclusion of BIC in December, 2013. There is a need to focus on the ways and means to achieve their sustainability, by involving the right stakeholders from the research communities, funding and implementation bodies (Government & Industry) in all countries. The EWG is an important concept and the EWG bodies should not be allowed to disintegrate and stop functioning after the conclusion of the BIC project as these working groups can provide very valuable inputs to the upcoming Horizon 2020 programme, and potentially other research programmes as well.

In summary, for the fulfilment of a longer term strategy of having multi-lateral cooperation in trustworthy ICT across multiple countries, it is highly recommended that the IAG and associated in-country bodies like the EWGs should be in a position to continue into the future and the countries programme management should work together on making this happen as a matter of urgency.

A recommendation related to the sustainability of the EWGs can be found in the next tactical recommendation.

TR2 The EU and BIC countries should formally recognise the Extended Working Groups as the nodal in-country agency/body to be actively involved in future H2020 (and beyond) international cooperation activities.

Rationale TR2.1 Although the EWGs in the BIC countries have been launched and currently running with a lead researcher in place, and enthusiastic researchers, the EWGs are still in stabilisation mode, looking at ways and means to sustain their activities.

To assist in receiving the required recognition of their efforts, the EU should take the opportunity to formally recognise the EWGs as a body in order to encourage the Governments of the participant countries to recognise them and help in allocation of funds to respective EWGs. Some avenues of support measures and mechanisms for their sustainability could include:

1. The partners of the BIC project will, of course, assist in each and every way possible to ensure their sustainability and look for other means and mechanisms to continue this important activity. For example, the BIC Web site, LinkedIn Group, and Wiki site will continue to be maintained for at least five more years to come and a number of the BIC partners have committed to continue in a personal capacity for as long as possible under their existing activities.

2. EWGs should look at establishing a formal government sponsored Centre of Excellence, which could facilitate sustainability, resources, and the infra-structural components required to continue.

3. The formal acceptance of EWGs as the nodal in-country agency/body and/or recognised “one stop shop” to promote and implement the BIC objectives of “International Cooperation for Trustworthy ICT” would greatly enhance their position and recognition.

4. Formal identification of three key stakeholders under the EWG forum vis. Research Institute, Industry and Government. The Government may identify a specific Ministry / Government Departments and notify the specified agency with their role for the purpose.

5. The objective, role and scope of EWG should be formalized in accordance with the details as stipulated in the earlier launch event reports pertaining to EWG formation and subsequent reviews, which has been agreed and ratified by the participating governments. These are summarised in recommendation number TR3.

6. Rules of governance and corresponding procedures should be evolved and formalized. An empowered EWG Steering Committee may be formed with one or two representatives each from: Research fraternity, Industry members and Government with a steering Head. These rules and procedures should be formed with a view to address the smooth functioning of the EWGs in accordance with the entire range of objective, role and scope of EWGs as duly defined.

Rationale TR2.2 The EWGs should not be in a position in which they will function in isolation.

If the EWGs find themselves in a situation where they are operating in isolation, they will disintegrate rapidly. To avoid this, the EU Commission should run H2020 workshops in each

country with the view to having a joint call in H2020 for each country. In each case, the EWG from each country should be invited to participate to play an active role, preferably as organisers. This will give a strong impetus for other organisations to participate in the EWGs from both the research and industry communities.

To this end, we feel that a BIC-IAG- like "overall coordination structure" would still be necessary as a driving force *and someone from the EU Commission should be appointed to be responsible for direct liaisons with the on-going IAG-EWGs*. This person should be thoroughly familiar with the work of the bodies and be appointed for a fixed duration, without interruption or continual changes, which results in dilution of the on-going relationships. Unfortunately, this has been an issue within BIC, whereby it was quite difficult to secure the same EU Commission representative each time at the meetings. The EU delegation members within the participating countries should also be appointed to play a key role in this on-going relationship between the EU Commission representative in Brussels and the IAG-EWGs.

TR3 The EWG should draw up and formalise their terms of references / objectives in synchronisation with one another and get these ratified by their respective Programme Management / Governments.

Rationale TR3.1 Consistency of structure and terms of reference will make the in-country running and interactions between the other EWGs easier.

The objectives, roles and functioning mechanisms and process of the EWG be should be drawn up in detail with well-defined deliverables and timelines, which should be agreed with the EU and the equivalent participating countries Programme management departments. This should be formally followed with a signed MoU. The EWG should, in general, for a start undertake the following:

a. Develop a plan for regular EWG Interactions: EWGs of the countries should hold regular teleconferences and events/ meetings together for exchange of research and development ideas and discussing issues.

b. EWG leads to discuss with local funding bodies regarding funding for future EWG activities, events or even bigger goals like setting up a Centre of Excellence to facilitate the EWG;

c. EWG leads to discuss the government plans for helping their country participants to participate in H2020, especially given the removal of the automatic funding clauses in H2020 from a number of the countries, including those within BIC.

d. EWG leads should continue and foster strong relationships with EU delegation members in their country;

e. EWG should organize regular workshops/symposiums/newsletters for dissemination purposes, for example, an annual congress of delegates for knowledge sharing and proceedings hosted by EWGs in rotation (similar to the recommendation about the IAG rotating ownership of responsibilities).

f. EWG should undertake collaboration with other relevant initiatives in the EU (e.g. NIS Platform – Europe, EU-India Working Group on ICT, EU-India WG on Cyber Crime, and

others) and within their countries of origin (e.g., Joint Working Group (JWG) on cybersecurity – India, Data Security Council of India, ORF/FICCI - Cy Fy annual conference, SBSeg, the Security research group of the Computing Society of Brazil, IBE (Instituto Brasil Europa), the Centre of Excellence in cybersecurity based at the Univ. of Johannesburg, and many others), thereby establishing a common platform for discussions and common sharable resource pool of research literature, projects knowledge repository and other resources.

g. EWGs should encourage strong collaboration with University members with activities such as Masters/Doctoral Programs, joint academic programs run by participating EWGs, scholarships/fellowships for students/faculty in these EWGs, exchange programs of student/faculty, sponsored school level competitions, and shared knowledge portal maintained for publishing research output/dissertations.

h. With regards to research and innovation of Horizon 2020: EWG should aim, plan and attempt how to attract and grow industry participation. (For example, this could involve building relationships with Industry bodies and having them join the EWGs, e.g. EU Technology platforms (ETPs) in EU, Brasscom in Brazil, FICCI in India, and others.) The EWGs should establish industry participation and development & innovation of researched products and solutions to the society as one of their key success metrics.

Rationale TR3.2 Expansion of coverage areas would widen the scope for participation to H2020.

Once the terms of reference and structures are in place for the EWGs, it should be fairly straightforward for the EWGs to undergo expansion on the topical coverage areas. The expansion of the EWG model into other domains to widen the potential coverage areas of H2020 should be encouraged from the outset.

There are a number of ways to effectively carry out the expansion to other areas, with identification of potential areas (those matching H2020 would be the most appropriate start), raising awareness activities, identification and recruitment of key experts from both research and industry and identification of the relevant funding bodies for these topics in the countries.

4.3 Properties of the ecosystem infrastructures and security exposures

SR6 There is a need to keep an international open-ness in specifications of services and standardisation

Rationale SR6.1 International interoperability (with diversity) to keep transversal applications and communications is a key principle. Interoperability does not mean unique implementation nor design

To promote international exchanges, it is necessary to preserve transversal properties across the ecosystem, that is to say, openness and interoperability of communications, calculations and storage, versus time and space. This does not mean that the whole system becomes transparent as free software or even with a uniform implementation. Openness means that the service, proprietary or not, must have known public interfaces so that it can interwork through it interfaces. Interoperability means that two services may be different, but they can inter-work together.

Openness and interoperability compromise the security of the entire ecosystem, as it becomes more vulnerable from its specification. Countermeasures to allow transversality are appropriate controls (identity management, protection mechanism of intellectual property, modern cryptography) under the form of technological protection measures (engineering mechanisms, biometrics, trust instrumentation) and under the form of international legal means for establishing trust between all actors at all scales, global, continental, national and regional scales.

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.

Rationale SR6.2 There is a need for international transparency (with the contradiction issue between visibility and trust on one hand, and anonymity, privacy or confidentiality, on the other hand)

Open Source

Open source plays an increasingly important role in the software and communications industries. Open source implementations are widely available for most of Internet protocols, from TCP/IP in kernel space (such as Linux, Android and BSD-based systems), down to MAC/PHY in hardware such as Ethernet and WLAN transceivers, and up to applications in user space such as WWW clients, servers and proxies. Hundreds of open source networking packages have played important roles in our daily life. The same open source spirit also goes to the development platforms for simulation, rapid prototyping, software defined radio, and software defined networking.

Open Data

The opening of data has been hailed for its innovative capacity and transformative power. Over the last years, many politicians, companies, scientists, and citizen communities have paid considerable attention to the demand of opening data of both public and private organizations. An important event in this context was the release of the EU Public Sector Information directive in 2003, in which a common legislative framework was presented, which regulates making data of public sector bodies available for re-use. In 2009, the US Administration stated that its primary goal was the establishment of an unprecedented level of openness of the Government and published an Open Government Directive. Building on former policies, the European Commission has presented an Open Data Strategy for Europe, in which more evident rules on making the best use of government-held information are presented. In 2012, the US Administration published the Digital Government Strategy, which aims to 1) enable the American people to access high-quality digital government information and services anywhere, anytime, on any device; 2) seize the opportunity to procure and manage devices, applications, and data in smart, secure and affordable ways; and 3) unlock the power of government data to spur innovation and improve the quality of services for the American people.

In addition to these policy documents, various studies have shown that opening data by public and private organizations has considerable potential to provide citizens, researchers, companies and other stakeholders with many advantages, such as a growing economy by stimulating innovation, developing new businesses and obtaining new insights in the public and private sector by creating new ways of understanding problems and interpreting data. Open data enable new ventures to develop new business models and innovative services. Often the added value is generated from combining multiple sources. Open data have the potential to enable different types of innovation, such as innovation through the provision, processing and use of open data, innovation through open data technologies, and innovation through impact and public value creation from open data initiatives (transparency, accountability and collaborative governance approaches). Open data can contribute to open government. However, although open data research is performed increasingly, research about the way innovation can take place through open data is still lacking.

Transparent Computing

Computing paradigms have greatly evolved with the rapid advances in hardware, software and networking technologies. Transparent Computing (TC), as a user-controlled cloud computing, is an emerging technology with the features of streaming-based scheduling and execution, user orientation, and platform independence. TC enables users to accomplish local tasks efficiently and flexibly through any type of devices while demanding computing and storage services residing in remote servers. Typical TC applications, such as transparent regional medical information sharing system and transparent campus information system, need to use the high performance computing technology to share the computing tasks of terminals. Furthermore, similar to Internet of Things, TC adapts to heterogeneous networks and protocols in order to make people enjoy intelligent services, anytime and anywhere. Finally, security and reliability is a crucial issue to the success of TC.

SR7 There is a need for an international mobility model approach

Driven by the ever-increasing popularity and demand of multimedia contents, wireless traffic is expected to increase by 1000 times in the next 10 years. These existing networks operate independently but will converge. There are security issues related to interworking of different types of networks, with a huge traffic.

There is a need for an international mobility model approach to deal with global traceability and anonymity (of digital events and people) due to the dissolution of spatial dimension (the paradox of the disappearing geography for international transactions and strengthening of finding location information for people)

Rationale SR7.1 It is necessary to solve issues of transcendence of borders, interconnection and interactivity of the borderless ecosystem

The digital ecosystem usage is international, but laws are national. There is a need to solve the non-overlapping of the virtual territory with digital entities and events, and the geographical territory of countries with national laws.

The world is changing at the speed of information and communication technology, resulting in all continents in an inevitable progress: billions of people can connect to a mobile phone and can access the internet. Digital infrastructures are becoming the backbone of technological and the economy progress. The digital world (Internet, mobile Internet, Internet of things, social networking, distributed software, embedded computing) is a space of technical and social innovation, and a space of relationships and interrogations, at all scales global, continental, national and regional.

Thus, cyberspace is a world without borders where individuals, businesses and things are interconnected in real time, with the ability to share and store large amounts of data and perform calculations on data. Many services in cyberspace are available to network users to process data. The relationship production-consumption of content or service has changed, so that everyone can be a producer, although the gap between internet giants and regular user has considerably widened.

Rationale SR7.2 In a borderless world, exploitation of non-overlapping geographical and digital boundaries by users and service providers is dramatically increasing

Attacks against national and private interests in the borderless realm of cyberspace over the past few years have spurred international efforts to defend critical information infrastructures. Some of the triggering events have included the "denial-of-service" attacks against Estonia in 2007[10], growing concerns about the "digital espionage" capability of certain nations, and the online targeting of corporate intellectual property, classified government information, and the financial interests of companies and individuals alike.

The competition between large groups is internationally fierce. The transversal property of cyberspace through the various continents, allows the exploitation of diversity and variable

[10] gainhttp://www.rand.org/pubs/periodicals/rand-review/issues/2013/summer/cybersecurity-strategies-raise-hopes-of-international-cooperation.html

maturity of countries vis-à-vis the consideration of digital questions: as finance invented tax havens, the digital ecosystem has its digital paradise where laws can be subtly used.

The multiplicity of motivations (ideological, political, religious, fraud, etc.), spontaneous and borderless nature attacks makes the challenge of security increasingly difficult. Atomization of attackers, their ability to unite and pool their efforts on the international stage, is becoming a growing concern for governments, especially when these groups are supported covertly by other governments. The defensive and offensive struggle of various countries also becomes a sovereign priority for peace in the world. The Cold War turned into a virtual latent conflict and moved into cyberspace, as an ideological and economic war.

Rationale SR7.3 Mobility, location and mobile computing will increase in the next decade

Mobile Computing and Ubiquitous Networking focuses on active areas of research and development in mobile communications, applications, algorithms and systems, as well as ubiquitous services and networking. Examples of such technologies include human-centric sensing, analysis and applications, mobile and pervasive healthcare, public and intelligent transportation and mobility, energy-efficient mobile systems, social-networking, machine-to-machine communications and their applications, mobile cloud computing and mobile social P2P, where human, machine, energy and environment are involved and tied closely with mobile and pervasive technologies for better urban lifestyles.

Rationale SR7.4 The increase of vehicles, robots, drones will raise a lot of security and responsibility issues

Over the last few years, significant efforts are being carried out by industry, academia and government agencies to improve driving safety, increase vehicle traffic efficiency and decrease fuel consumption by exploiting vehicular communications and networking technologies. These technologies, which are generally referred to as VANET (Vehicular Ad Hoc Networks), include Vehicle-to-Infrastructure (V2I), Vehicle-to-Vehicle (V2V) communications and can be based on short- and medium-range communication as well as on cellular systems. They promote further research activities on services such as; advanced traffic management, safety control, comfort applications and networking and information services for users on the road.

SR8 There is a need for an international approach dealing with the massive abstraction of software and data (e.g. resilience of virtualisation, security of Big Data)

Rationale SR8.1 The massive concentration of computers (High Performance Computing, Cloud Computing) bring new challenges in security, trust and privacy (authentication, protection of personal data, cryptography)

With the rapid growth in computing and communications technology, the past decade has witnessed a proliferation of powerful parallel and distributed systems and an ever-increasing demand for practice of high performance computing and communications (HPCC). HPCC has moved into the mainstream of computing and has become a key technology in

determining future research and development activities in many academic and industrial branches, especially when the solution of large and complex problems must cope with very tight timing schedules.

Cloud Computing systems offer users flexible accesses to computing, data resources, communication networks, services, and applications. The increasing deployment of cloud applications has created demands for designing a reliable, secured, and efficient cloud system. Cloud applications come with various needs. Some cloud applications require intensive computing resources, while others may emphasize on data storage and with a certain level on data protection. Therefore, it is challenging to design a cloud computing system that can meet various requirements from diverse cloud applications and services.

Rationale SR8.2 The increased concentration of personal usage (Online Social Networks) has changed the whole security view of internet in the past ten years, and this trend will continue

Social network analysis and cloud computing are two of the most exciting new trends in the recent developments of ICT. As the new generation computing paradigm, cloud enables computing resources to be provided as IT services in a pay-as-you-go fashion with high efficiency and effectiveness. With the popularity of social software as well as the fast development of cloud and other high-performance computing infrastructures, the outcome of social network analysis is becoming more and more attractive. However, information privacy and security issues are major challenges in both these areas.

In the current Internet, important new overlay and cloud applications significantly influence volume and patterns of Internet traffic. While overlay applications such as Content Delivery and P2P store and circulate information among each other with no awareness of the topology and state of the underlying transport network infrastructure, cloud applications delegate storage and computation to the network, which is valuable for devices with limited resources and access. At the same time, online social networks (OSN) like Facebook gain more and more popularity and attract millions of users. The widespread adoption of OSNs has drastically changed the way content is consumed in the Internet, as content consumption is nowadays highly impacted by the information shared by users through OSNs and the popularity of a given content is most often dictated by its "social" success. In turn, the adoption of socially-aware traffic management mechanisms as a new management approach allows for a tighter integration of network management and overlay service functionality which can lead to cross-layer optimization of operations and management, thus, being a promising approach to offer a large business potential in operational perspectives for all players involved. This approach shows benefits for overlay and cloud applications and services which are currently dominating Internet traffic, but still have a large potential for optimization, e.g. in terms of security, privacy, energy efficiency, inter-cloud traffic.

SR9 International cooperation is needed to deal with the fragility of interconnections

Rationale SR9.1 Resilience of ecosystems/infrastructures is an essential requirement

The development of modalities for international cooperation for cybersecurity is the cornerstone of global security of digital ecosystem: cyber defence can never be effective without having an international dimension. 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). Dialogues, and consolidation at the international level, are important to validate the interoperability issues. A comprehensive policy of reliability and security management is essential to protect this vital infrastructure, equipment and network services. A global security policy is essential for securing software and data: it is personal data of individuals or companies, and software of vendors and service providers. Governance of the ecosystem between all stakeholders is to strengthen, at the scale of the global challenge, because the information sharing and cooperation are the basis for the construction of this digital ecosystem.

Rationale SR9.2 There is a need to renew the vision of security of the future internet

The technological evolution of the future Internet must take into account the new security requirements. The relationship with the physical world must also be taken into account, since the digital ecosystem is increasingly entangled with the real world: ethics of robots and drones, security of interconnected objects of IoT, security policy of distributed applications (M2M), identity management, data and software worldwide security, security policy for the execution of cross-border services, security of virtual entities, security policy of cross-border mobile applications, security policy of services and data, and crisis management, outside the country where the responsible stands.

Rationale SR9.3 Services must be reliable so that users have confidence

Robustness of services, reliability of infrastructures, protection of consumers and citizens, respect of user's privacy, management of digital identities and users' confidence in the whole system are essential for the sustainability of the ecosystem. People do not want their digital behaviour to be snooped to, that their personal data becomes a commodity without their explicit consent. People claim a right to be forgotten for data stored too long. Users appreciate anonymity of the network but want fraud by impersonation is fought. Companies want to relinquish them too cumbersome information system, using the intermediation of cloud computing. But companies want to preserve the sovereignty of their digital industrial heritage. In addition, users also demand a green digital ecosystem where energy efficiency is implemented.

Rationale SR9.4 Cyber Physical System (Smart grids, smart metering, smart cities) are realized in everyday life and in the urban environment with quantitative records, questioning privacy

Smart grids will be deployed in the coming years to improve the multi-source power supply, by association of electrical networks of production and distribution and ICT networks, in order to adjust production and consumption energy. This new digital integration in electricity infrastructure introduced unprecedented vulnerabilities, both in critical infrastructure (cyber-terrorism to destabilize countries) and households (by cyber fraud and breaches of privacy). Investment security should reach 15% of the total investment. Smart Grid Communication technologies capable of enhancing energy efficiency, utility operations, renewable resource integration, and meet the needs of increasing power demands will lead the global evolution of the Smart Grid. Managing data, leveraging new opportunities in M2M, and delivering a robust and secure infrastructure are paramount responsibilities for both communication and data service providers in the European landscape, as well as key in all future and existing deployments in the European Market.

Rationale SR9.5 The emergence of Internet of Things will modify the security issues in terms of responsibililty

Technologies such as RFID, sensor networks and NFC are bringing the vision of the Internet of Things, intelligent data-enabled devices connected to the pervasive internet infrastructure, closer to reality. Creating the Internet of Things has many emerging challenges: the integration and management of heterogeneous data, the integration and transfer of enriched data, the effective use of knowledge-based decision systems, retrieval and sharing of knowledge automatically from huge volumes of data, ensuring security and protecting privacy. NFC technology enables communication in close proximity within a few centimetres. Today, one million NFC smartphones are sold every week. With NFC mobiles surfacing the market so quickly, mobile operating systems are prepared for support with dedicated frameworks. This offers researchers and developers a great opportunity for getting quick traction with novel applications. So far, the main NFC-enabled services deal with payment, access control, or ticketing. Commercial applications today mainly target contactless payments, managed by transportation companies. The broad availability of NFC-technology fertilizes research and development of novel applications and can go well beyond these intended applications.

Rationale SR9.6 Security also covers SCADA, Embedded Computing as autonomous systems, protected from real time network connections, can also be attacked

Embedded and ubiquitous computing is an exciting paradigm that promises to provide computing and communication services to the end users all the time and everywhere. Its systems are now invading in every aspect of our daily life and promise to revolutionize our life much more profoundly than elevators, electric motors or even personal computer evolution ever did. The emergence of this technology is a natural outcome of research and technological advances in a variety of areas including embedded systems, pervasive computing and communications, wireless networks, mobile computing, distributed computing and agent technologies. But security also covers SCADA or embedded system as

autonomous systems, protected from real time network connections, can also be attacked (e.g. severe attack on Iranian nuclear plant).

4.4 Properties of the ecosystem usages and weaknesses

Challenges of network security come in many forms. Globally, accidents, failures and attacks that affect the entire infrastructure must be limited. These are essentially cascading effects that cause denial of service through overloads, and can interrupt the service continuity in a large part of the ecosystem. In terms of misuse, networks are essentially prey to fraud and identity theft for e-commerce, or identity theft or defamation for social networks, which sometimes lead to tragic dramas. The theft of intellectual property in software, multimedia content, for personal or business data harms business competitiveness and the creation of digital entrepreneurs.

SR10 We need an international (or harmonised) approach to steer the evolution and strengthening of the digital ecosystem in terms of network security governance and surveillance

Rationale SR10.1 Interdependence of infrastructures, individuals, enterprises and states must be monitored

Individuals and businesses are increasingly dependent on these infrastructures. Economy, culture, research is dependent on our relationship with these infrastructures. Digital technology is a technology that abolishes distance and time, which stores for many years all data. It provides immediate access to information and knowledge, and it also allows to expressing themselves anonymously or not, public or semi-public, in real time, with forums, micro-blogs, websites and social networks. Digital technology transforms society, economy, social links, and cognitive sources of human beings. Mutations are affecting education, health, public services, transport, industry, business, networking, finance, how to be a consumer and how to be a citizen. Knowledge through this information from various sources and of various qualities is a permanent concern.

Rationale SR10.2 Models of asymmetry and feedback loop phenomena must be searched at the international scale

Communities and pressure groups formulate different strategies to maximize their presence on the internet. The asymmetry of the fight in cyberspace is an essential property: governments dealing with cybercriminal, or large groups dealing with user. The digital ecosystem is also an amplifier in terms of exposure of private life, crowd behaviour and communities of all kinds, of disinformation and manipulation of any kind. Asymmetry is erected in this ecosystem, between one user and the rest of the system, with its opportunities, but also its threats. An unequal face-to-face presence appears between the digital ecosystem as a machine and a practice that obtrude oneself on the user on the one hand, and the user fully responsible for his actions on the other. The user is hard to defend himself in front of the stakeholders in the network (operator and service providers) that weigh their heaviness, and other users of the network, unknown docile or anonymous attackers. Individuals, small businesses, large groups and governments are forced to consider or comply with the cyber-social meta-running system. Moreover, petty criminals, organized

crime groups and terrorist organizations have gained a large area where they can exchange secretly or anonymously. But social movements and political expressions are also expressed through this medium. Social networks and cyber-activism are two major phenomena of free expression in recent years. The sounding of these expression media influence or shakes all governments. If countries are democratic, governments are obliged to take account of repeated attacks of these expression movements. If countries are not democratic, these new digital services become a weapon to people in countries where freedom of expression is not easy.

Rationale SR10.3 Anonymity within networks, vector of freedom, implies major threats, versus Identity

Anonymity is the major support of these threats, which has its effects amplified by the low cost of Internet presence. Microblogs, blogs, websites, forums intervention are within the reach of all of us. Rumour, defamation, disinformation, media lynching are difficult to fight legally. Anonymity, dynamicity and mobility in cyberspace and trans-boundary aspects allow criminals to act from country refuge, or organize a crime market: information gathering, marketing of personal data, credit card data, and sale of viruses or botnets on the black market.

Rationale SR10.4 Network management, governance, surveillance or control must be discussed, analysed and clearly specified

Threats to the ecosystem have two forms. Following a technically normal use of networks, threats lie in the content of provided information, or, following misuse or exploitation of system vulnerabilities, threats lead to system malfunction. The security policy must take into account these two aspects, where network monitoring may appear as abusive surveillance. How to monitor the network infrastructure and information flows, either in form or in substance, and the intensity of this monitoring, pose ethical questions about freedom, which are not resolved today. In many countries, heavy surveillance of network usage, excessive filtering on information flows, overzealous censorship on the content, use of personal data without the consent of individuals, calculations on metadata of communications and applications, are far beyond the legitimate limits. The global security policy must take into account both usage and infrastructure, in order to preserve innovation, and openness and freedom values of our society. This security policy should not slow the momentum of the Future Internet development.

Rationale SR10.5 International governance must be addressed seriously and without taboo: governance of the ecosystem is an international concern and must be apprehended in a multipolar aspect

In the future during Horizon 2020, smart grids, smart cities, the Internet of things, administration, education, health, will deploy more and more to switch the classic urbanization of our cities into a wide cyber-social meta-system in command-control with digital networks. All these vital infrastructures (water, energy, finance, transport) will depend on these calculations and distributed computing and the generalized interconnection. Relationship with the ecosystem, governance type of the ecosystem, transparency between

all stakeholders (governments, service providers, users), mode of resource protection of these actors, potential for evolution of this ecosystem, competition between suppliers, system monitoring are essential so that everyone benefits from technological progress.

Threats in terms of confidentiality (spying on the data stream, attacks on cryptographic mechanisms, diverted use of personal data) in terms of falsification and alteration of industrial systems (attack by terrorist groups or rogue nations, cf. Stuxnet worm), in terms of availability (denial of service of control-command network, vandalism of deployed infrastructure, falsification of smart meters) already exist and have high risk and high impact. The preparatory work of the European Commission on the subject is insufficient, and research must be addressed at the international level to place Europe at the forefront of these technologies: protection of critical infrastructure, security of personal data on smart meters and all the subsequent chain to respect privacy of consumers and citizens, privacy and trust models, and identity frameworks.

5 - Priority topics and roadmap for international cooperation in Trustworthy ICT

This section gives an overall overview of the general topics in security research at the international level that Europe should push forward in order to reach a sound level of trustworthiness, at the Horizon 2020, in cooperation with the other continents. These topics 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.

5.1 Priority topics for international cooperation in security research

Table of the ranked priority research

Following the description, analysis and the mapping exercises of the Deliverable D2.4 (see Annex 1 and Annex 2) of the research priorities, the following topics have been identified as a first list of potential topics by the EU and Brazil, India, South Africa researchers for mutually beneficial cooperation in the area of trust and security. They are grouped in six general themes as shown in table 1.

Table 1. Table of the ranked priority research

Topic 1 : Cybersecurity
Fight against cybercrime, digital forensics, move from bilateral approaches to multilateral approaches, critical infrastructure protection;
Topic 2 : Trust and Privacy
Trust instrumentation, human values, social computing trustworthiness, privacy by design, information security awareness;
Topic 3 : Mobile security, Social media and Cloud security
For individuals and enterprises, standardisation and metrics, software security;
Topic 4 : Security of Applications and data protection
Ownership, intellectual property, data provenance, digital governance, usage control, Big Data;
Topic 5 : Identity management, accountability frameworks
Strong authentication, forensics, responsibility, digital evidence, digital signature, certificates, usage control;
Topic 6 : Future Internet security
Security of the Future Internet (network security and information security), cryptography and protocols, security of smart grids, of IoT, robots and drones, green security, search engine.

We can also summarise these topics around key challenges of the Future Internet at the Horizon 2020 as shown in table 2:

Table 2. Table of key challenges of the Future Internet at the Horizon 2020

Diversity and interoperability An ecosystem in the global geography with diversity of cultures and contexts;
Flexibility and innovation An ecosystem flexible, simple, universal and polymorphic in its structure, sharpened and adjusted in usage;
Trustworthiness Strengthening the resilience of infrastructure control and crisis management;
Transparency Governance and digital control, in Europe and worldwide and digital multilateral governance at global scale, neutrality of the entire ecosystem, not just net neutrality;
Freedom, Openness, Ethics Principles of human values, flexibility and usability, architecture and usage interrelation and feedback, building together a cyber-ethics;
Accountability and Responsibility Digital sovereignty of responsible entities (providers, users) and the redefined responsibilities of access, services, content providers, and digital dignity of users, and respect for privacy and digital behaviour;
Trust and Privacy Digital industrial policy, restoring confidence and privacy, intimacy of cloud computing, repositioning trust infrastructure at the same level as security infrastructure.

Priority research at the Horizon 2020

In the Deliverable D3.1, we already listed a set of long-term recommendations (2015-2020) – these can be found summarised in Annex 3. The mapping between these previous priorities and the long-term recommendations may be grouped according the following partition as shown in table 3:

Table 3. Table of priority research according society, technology, legislation and governmental issues

- **Societal:**
  - Cybersecurity: Training of the stakeholders requires cyber defence exercises;
  - Trust and Privacy : User awareness, personal data protection; human values;
  - Mobile and Cloud security : new business models;
  - Security of Applications: Digital governance;
  - Identity and Accountability : Social computing awareness; Usage control, Big Data security;
  - Future Internet security: Usability, user-centric approaches, green security.
- **Technological:**
  - Cybersecurity: New traffic management models, Digital Business Models, Evolutionary integration models;
  - Trust and Privacy : Universal trust models, accountability and responsibility;
  - Mobile and Cloud security : Operating system security, Operating permit to cloud service operators, Risk metrics for cloud usage;
  - Security of Applications: homomorphic cryptography, watermarking, IPR, DRM, Big Data, search engine;
  - Identity and accountability : Post-incident investigations adapted to the virtual world, Audit mechanisms for a virtual world;
  - Future Internet security : Network and Information security, engineering (biometry, etc.), cryptography, Technological support, secure managing and monitoring, green security, critical infrastructure protection.
- **Governmental:**
  - Cybersecurity: Resilience of cyberspace, Management of panic, Preparation for any adverse situation, Digital governance model, Cyber defence having an international dimension, Anti-cyber laundering initiative, Global data and information flow agreement, critical infrastructure protection;
  - Mobile and Cloud security : secure deployment;
  - Security of Applications: business model of the ecosystem, standardisation, governance, certification;
  - Identity and Accountability : Identity management, accountability frameworks, identity cards, digital signature, certificates, security assessment;
  - Future Internet: standardisation, governance, critical infrastructure protection.
- **Legislative:**
  - Cybersecurity : Demarcation of responsibilities for cyber-protection;
  - Trust and Privacy : Legal or constitutional changes to erect cyber deterrence;
  - Mobile and Cloud security : New business models with user's assurances;
  - Security of Applications: ownership, IPR, digital governance, digital evidence, usage control;
  - Identity and Accountability : Data ownership rules, Global digital dispute analysis and resolution framework, forensics, digital signature, certificates;
  - Future Internet: Cyber deterrence framework, PPP, private sector relationships.
- **Research organizational:**
  - All themes: Strategic global research frameworks in the H2020.

5.2 Roadmap for strategic recommendations

The following table 4 lists the different topics in security research to reach the recommendation targets, with an estimated timeline to start these studies.

Table 4. Table of strategic recommendations, rationale and estimated timeline

Recommendation	Rationale	What is needed	Estimated timeline
SR 1. Need for new global approaches and meta-models	SR1.1 Holistic global meta-models taking into account diversity	Experiments of new metamodels and simulations	2017
		New design paradigms for future network convergence, traffic metrology, worldwide measurements	2015
		International cooperation in network cryptography	2014
	SR1.2 Concepts to be expressed in computer science terms and instantiating cultures	Comprehensive secure SDN, recursive and/or fractal Internet, polymorphic models	2014
	SR1.3 Quantitative security assurance and trust instrumentation	Security methodologies based on scientific and quantitative foundations (trust measurements); standardisation and metrics, software security	2015
	SR1.4 Crossborder computing	Policies to integrate borderless aspects	2015
	SR1.5 Massive global networked phenomena	Sociological statistics in real time	2015
	SR1.6 The future Internet of Things	Models for the future Internet of Things	2015
		New security architectures, new global object identifications and new security models	2017
SR 2. Evolutive cybersecurity at the global scale	SR2.1 Borderless massive usage of the network, with crowd effects	Technology and policy to monitor traffic	2015
		Improvement of international legislations	2017
	SR2.2 International attackers	Global traceback of malicious flows; international data exchange for cybersecurity; sharing of information and intelligence on cyber-attacks	2015
		New models of threats; cybersecurity policy, digital forensics	2015
	SR2.3 Cyber-war between continents	Task forces for more transparency and for a better governance of the ecosystem	2017
	SR2.4 Non transparent worldwide surveillance of networks, and people activity	Policy for more transparency and for a better governance of the ecosystem	2018

Recommendation	Rationale	What is needed	Estimated timeline
SR 3. International cooperation research for H2020	SR3.1. Reliable and secure design of technology, under international supervision	International cooperation for global tools and protocols and for the international traffic; Future Internet (infrastructure, network, protocols, applications, services, information and data)	2015
	SR3.2. Use of existing structures for a resilient ecosystem	Discussions at the G20, UN, ITU, OECD, IETF and task forces to convince refractory states	2015
	SR3.3. Mitigate difficulties of international cooperation at the state levels	Definition of continental cybersecurity strategy, in concrete terms	2016
	SR3.4. Cybersecurity strategy at the global scale	Enforcement of continental cybersecurity strategy, in concrete terms	2017
SR 4.Agreement on grand principles	SR4.1 Ethical, legal and technological dimensions of trustworthiness	Principles of human values, flexibility and usability, architecture and usage interrelation and feedback, building together a cyber-ethics; Task forces for a minimum ethical platform; Human oriented security, security usability; Human value policy : Freedom, Openness, Ethics	2015
	SR4.2 Accountability versus responsibility of service providers at the global scale	New policies of copyrights of software and services	2016
	SR4.3 Diversity for privacy and responsibility	New models of privacy, accountability and responsibility (for ISP and for endusers)	2015
SR5. Shift to a multi-lateral approach for INCO.	SR5.1 Comprehensive spread of global participation	Continuation of european projects with USA, BRICS countries, Japan, Korea, Australia…	2014
	SR5.2 Bi-lateral INCO for cybersecurity	Global Frameworks for multi-lateral cooperation and international alignment	2015
SR6. Open-ness in specifications of services and standardisation	SR6.1 International interoperability	Curb the tendency to make the ecosystem, proprietary and opaque. Ecosystem models with flexibility	2014
	SR6.2 International transparency	Global cyber forensics; promote business models that use open systems and are transparent vis-à-vis personal data. Digital industrial policy, restoring confidence and privacy, intimacy of cloud computing, repositioning trust infrastructure at the same level as security infrastructure	2014

Recommendation	Rationale	What is needed	Estimated timeline
SR7. International mobility model approach	SR7.1. Borderless ecosystem	Models and experiments of virtualisation resilience	2015
	SR7.2. Non-overlapping geographical and digital boundaries	Policies for virtual plates and transboundary ICT	2017
	SR7.3. Mobility, location and mobile computing	Privacy of location; trust, security and privacy models in mobile environments; Social media and Cloud security	2015
	SR7.4. Vehicles, robots, drones	Ethical behavioural models of drones and robots	2016
SR 8. Massive abstraction of software and data (Big Data)	SR8.1 Massive concentration of computers	Strong authentication and authorisation; new cryptographic tools for cloud computing	2014
	SR8.2 Online Social Networks, security, trust and privacy	Security models of personal data; putting citizens in control of their data; protection of endusers against unfair ISPs, e-reputation models, universal trust models, security usability; social computing trustworthiness; Security of Applications and data protection	2015
SR9. Fragility of interconnections	SR9.1 Resilience of ecosystems/infrastructures	Exchange of cybersecurity information between countries (CERT), framework for international cooperation in cybersecurity; crisis management systems	2015
		New models and simulations to design and measure resilience of large systems. Critical infrastructure protection; crisis management	2015
	SR9.2 Renewal of the vision of security of the future internet	Stochastic approach of security of large systems	2017
		New Intellectual Property rights frameworks; ownership, intellectual property, data provenance	2017
		Security and privacy by design, development and operation	2014
	SR9.3 Reliable services	Prevention of attacks, security of payment, security enforcement tools; information security awareness	2014
	SR9.4 Cyber Physical System	New models of distributed privacy, smart grids, smart cities, smart metering	2015
	SR9.5 Internet of Things	Privacy kits at home to prevent intrusion or surveillance; New infrastructures to secure Things and to be protected from Things.	2015
	SR9.6 SCADA, Embedded Computing	Fast detections of attacks	2015

Recommendation	Rationale	What is needed	Estimated timeline
SR 10. Steering the evolution (network security governance and surveillance)	SR10.1 Interdependence of infrastructures, individuals, enterprises and states	Enhancement of interdependence simulators, green security (versus green networking)	2017
		Risk management (economics of security and privacy); responsibility, digital evidence, digital signature, certificates, usage control	2016
	SR10.2 Models of asymmetry and feedback loop phenomena at the international scale	Models of disconnection; Appropriate regulations	2017
		Sociological statistical frameworks (crowds)	2017
	SR10.3 Anonymity versus Identiy	Identity management; Identity frameworks (for persons, things and digital entities); Anonymity frameworks, Accountability frameworks; Digital sovereignty of responsible entities (providers, users) and the redefined responsibilities of access, services, content providers, and digital dignity of users, and respect for privacy and digital behaviour	2016
	SR10.4 Network management, surveillance or control	Global policy to manage and control ecosystems; digital governance, usage control	2017
	SR10.5 International governance	Multipolar frameworks of governance; Governance and digital control, in Europe and worldwide and digital multilateral governance at global scale, neutrality of the entire ecosystem, not just net neutrality	2018

5.3 Roadmap for tactical recommendations

The following table 5 lists the different topics in security research to reach the recommendation targets, with an estimated timeline for these actions.

Table 5. Table of tactical recommendations, rationale and estimated timeline

Tactical Recommendation (TR) name	What is needed	Estimated Timeline
TR1. The work of the BIC project and mainly its structural components (IAG, WGs) should be functionally sustained from the long term perspective of at least 10 years, and also expanded to other countries, especially in terms of the cooperation platform components - International Advisory Group, Core Working Groups and in- country Extended Working Groups.	TR11 In principle acceptance of this recommendation by EU and sending demand to BIC Project for submission of "BIC Continuity Proposal (BCP)" with specific requirements.	April 2014.
	TR12 BIC to submit above BCP with specific details about Role & Objectives, Deliverable, Project Plan Time Lines & costs. EU to make policy/ rule provisions for BCP under H2020.	June 2014.
	TR13Approval of BCP by EU and release of funds.	September 2014.
	TR14 Communication to other Country's Govts.	September 2014.
TR2. The EU and BIC countries should formally recognise the Extended Working Groups as the nodal in-country agency/body to be actively involved in future H2020 (and beyond) international cooperation activities.	TR21 Internal review of the concept by the EU and communication about the same to the other Govt bodies of BIC countries, seeking their comments and consent.	April 2014.
	TR22Formal Recognition of EWGs by EU	June 2014.
	TR23Formal recognition of EWGs by other BIC countries	September 2014.

Tactical Recommendation (TR) name	What is needed	Estimated Timeline
TR3. The EWG should draw up and formalise their terms of references / objectives in synchronisation with one another and get these ratified by their respective Programme Management / Governments.	TR31 IAG to prepare base document on Terms of Reference (EWG-TOR) covering their Role, Objectives and Deliverables and circulate to EWGs of the BIC countries and also to other prospective countries who need t become part of the BIC programme.	May 2014.
	TR32 All EWGs prepare their draft EWG-TOR around the base document of IAG, adding their country specific aspects and submit the same to IAG.	August 2014.
	TR33 IAG facilitates synchronisation of EWG-TORs amongst all countries and EWG TORs are formalised, agreed by all and published by IAG.	November 2014

Deliverable **D3.1 - Interim recommendations report on future global research challenges in ICT trust and security**, describes in detail, a considerable number of long term recommendations, or more appropriately, recommended actions to be taken in H2020, for the implementation of international cooperation and trustworthy ICT. In the interest of brevity, a summary of these recommended actions are set out in Annex 3. One of the main findings of D3.1 is that when the security of a system is analysed, it is necessary to first consider the security features that come with the system properties, and then to study the additional security features required to protect the system or the system users. These actions can be broken into the following forms:

- ✓ Actions related to the evolutionary properties of the ecosystem (such as digital business models, evolutionary integration models...)
- ✓ Actions related to intrinsic security functions (such as audit, contingency plans...).

When these actions are analyzed, we come to understand the urgency, by 2020, of achieving a new global initiative to manage and to govern the entire ecosystem with more quantitative indicators than currently used, both in technical terms (traffic,.) and in terms of the satisfaction of all users (trust of actors, ..). To achieve these goals, we must mobilise end users to increase their awareness of the need to protect themselves (end users and enterprises). It is also urgent to create an influential international Think Tank similar to the BIC IAG-EWG to move the lines on the global aspects. This Think Tank would be, with the help of an international research group, a little more open and less technical than the IETF.

We also understand that many actions are societal and cultural and relate to the law at a high level: the concepts of ownership, human behaviour, insurance with respect to its heritage, etc. They cannot be resolved into a rigid framework with a single technical solution. It is, therefore, urgent to establish an international working and harmonisation group to extract the greatest common factors to unite the approaches of the different continents.

In the current H2020 calls, it is not clear if this global vision and global scale are taken into account as many of the International actions are relegated to the second call. It is essential for Europe to create at the earliest opportunity, calls for proposals in the framework of international cooperation, to reconcile points of view on a continental scale.

In this deliverable D3.2, BIC further distils and prioritises the recommendations and topics and undertakes a mapping of the Strategic recommendations to these topics. Table 6 presents the final ranked recommendations (SR1,..,SR10), the important recommended actions distilled from Annex 3, their estimated timelines and an indication of where they could potentially fit within the H2020 programme. A similar mapping of the Tactical Recommendation to H2020 has not been done since the first call of H2020 does not include International cooperation actions[11]. It is important to note even for the SR's mapping, this correlation process proved difficult due to the absence of options for international cooperation in the first call of H2020. In terms of the timings, we estimate the year(s) in which results can be expected, dependent on the published work programme calls for H2020. The convention used for timings is the following:

- Action addressed in call 1 of H2020 (deadline April, 2014), results emerge in 2016;
- Action addressed in call 2 of H2020 (deadline c. August, 2015[12]), results emerge in 2017;

[11] We feel this matter will need to be addressed with the government bodies (EU and others) to accelerate the Tactical Recommendations take-up in the absence of international actions in call 1 of H2020. In D2.5, Final report of the working groups, we also give further suggestions for how the BIC IAG and EWGs should continue.

[12] As announced at the INFO Day on 15th Jan. 2014 on Trustworthy ICT

- An action addressed in both calls 1 and 2, results will begin to emerge in 2016/ 17;
- An action that cannot be addressed in either call 1 or 2, rmay be included in call 3 with results beginning to emerge in 2018-2020.

Table 6. Timeline of strategic recommendations (see Annex 3)

Estimated timeline to realise international cooperation on key topics		
Topics towards harmonisation, openness and interoperability, taking into account the expansion and complexity of the ecosystem, diversity of cultures and usage, and human aspects		
SR1	Concepts to deploy a global ecosystem: design of models, metrics, tools and mechanisms	
	2017	**Digital business models** to promote entrepreneurship in the digital world, **evolutionary integration models** for the ever-expanding and virtually limitless expansion of the digital world. Fit in H2020: Call 1 ICT 5 – 2014: Smart Networks and novel Internet Architectures ; ICT 1 – 2014: Smart Cyber-Physical Systems ; ICT 11 – 2014: FIRE+ (Future Internet Research & Experimentation)
SR3	2016 - 2018	Establishment of some **universal trust models**. **Risk metrics for cloud usage** for individuals, for businesses, and for administrations. Fit in H2020: Call 1 ICT 7 – 2014: Advanced Cloud Infrastructures and Service, including Security. Call 2 EU - Brazil call, EUB 1 – 2015: Cloud Computing, including security aspects.
SR5	2016 - 2018	Development of some **suitable governance model** with necessary powers for the governors. Fit in H2020: ICT 14 – 2014: Advanced 5G Network Infrastructure for the Future Internet; ICT 16 – 2015: Big data – research; ICT 17 – 2014: Cracking the language barrier
SR6	2017	The flow of data and information across the geopolitical borders require some **global flow agreement** to facilitate the export control. Fit in H2020: ICT 38 – 2015: International partnership building and support to dialogues with high income countries ; ICT 39 – 2015: International partnership building in low and middle income countries
SR8	Instructive and informative actions to enhance education and research: design of education, training and research programmes	
	2016 - 2020	**User awareness programmes** for different but overlapping groups of society, and **cyber defence exercises** for stakeholders involved in the digital ecosystem. Fit in H2020: ICT 38 – 2015: International partnership building and support to dialogues with high income countries. ICT 39 – 2015: International partnership building in low and middle income countries. Note 1. Cannot find an exact fit in calls 1 or 2, except for international partnership building and support to dialogue as above. Note 2. This should be done in conjunction with the ENISA cyber exercises and other national exercises that are held (e.g. Ireland, France, etc.).
	2016 - 2017	Strategic **global research frameworks** should be enabled in the H2020 funding mechanisms for multi-lateral cooperation. Fit in H2020: ICT 38 – 2015: International partnership building and support to dialogues with high income countries; ICT 39 – 2015: International partnership building in low and middle income countries.

Topics towards security, protection, crisis management, taking into account complexity, interoperability, and scalability and multidisciplinary aspects			
	Technology to increase trustworthiness: models and tools		
SR2 SR3	2016	Development of **audit mechanisms** and digital investigations tools for a virtual world, within the context of globalisation of criminals and their targets. Fit in H2020: ICT 32 – 2014: Cybersecurity, Trustworthy ICT; ICT 9 – 2014: Tools and Methods for Software Development Call – Digital Security: Cybersecurity, Privacy and Trust DS-1-2014: Privacy; DS-2-2014: Access Control; DS-3-2015: The role of ICT in Critical Infrastructure Protection; DS-4-2015: Secure Information Sharing	
SR4	2016	Development of new **traffic management models** to deal with 'rush hour' flow management especially in the advent of emergencies. Fit in H2020: ICT 32 – 2014: Cybersecurity, Trustworthy ICT;Call – Digital Security: Cybersecurity, Privacy and Trust; DS-3-2015: The role of ICT in Critical Infrastructure Protection; DS-4-2015: Secure Information Sharing; DS-5-2015: Trust eServices	
SR5	Continuity of service: contingency plans		
SR7	2016	Development **of contingency plans** to avoid alarm in the case of any high profile cyber incidence, and preparation for any adverse situation to cope with the aftermaths of a possible outage or serious depletion of digital resources. Fit in H2020: DS-6-2014: Risk management and assurance models	
	Legal actions: enhancement of legal framework and design of institutional observatory		
SR8 SR9	2017	Implementation of a **cyber-deterrence framework**, and modalities including legal and constitutional implications. Fit in H2020: ICT 39 – 2015: International partnership building in low and middle income countries. ICT 39 – 2015: International partnership building in low and middle income countries.	
SR10	2016 - 2017	Design of **data ownership** rules, of **transparent cyber-policing rules** including virtual border-controls, of a **global digital dispute analysis** and resolution. Fit in H2020: DS-1-2014 : Privacy; FCT-1-2015 : Forensics topic 1: Tools and infrastructure for the fusion, exchange and analysis of big data including cyber-offenses generated data for forensic investigation.	
	2017	An **effective anti-cyber laundering initiative** will deter criminals and help authorities to identify new kind of frauds. Fit in H2020: FCT-4-2015 : Forensics topic 4: Internet Forensics to combat organized crime.	

Mapping recommendations with H2020 calls

Calls for proposals in H2020 have been published for 2014 and 2015 and the most relevant for the work of BIC can be found in 5. Leadership in enabling and industrial technologies (LEIT), i. Information and Communication Technologies[13], and 14. Secure societies – Protecting freedom and security of Europe and its citizens[14].

As shown in Table 6, a number of calls related to these recommended actions and their mapping to the ***Strategic recommendations*** are identified. It is interesting to note that some calls have technical or social trends. Some calls explicitly have an international vision and a global scope, others are bi-lateral cooperation (Brazil, Japan). The most related calls identified are the following:

- ICT 1 – 2014: Smart Cyber-Physical Systems
- ICT 5 – 2014: Smart Networks and novel Internet Architectures
- ICT 7 – 2014: Advanced Cloud Infrastructures and Services
- ICT 9 – 2014: Tools and Methods for Software Development
- ICT 11 – 2014: FIRE+ (Future Internet Research & Experimentation)
- ICT 14 – 2014: Advanced 5G Network Infrastructure for the Future Internet
- ICT 16 – 2015: Big data - research
- ICT 17 – 2014: Cracking the language barrier
- ICT 30 – 2015: Internet of Things and Platforms for Connected Smart Objects
- ICT 32 – 2014: Cybersecurity, Trustworthy ICT
- ICT 38 – 2015: International partnership building and support to dialogues with high income countries
- ICT 39 – 2015: International partnership building in low and middle income countries
- EU-Brazil Research and Development Cooperation in Advanced Cyber Infrastructure
    - EUB 1 – 2015: Cloud Computing, including security aspects
    - EUB 2 – 2015: High Performance Computing (HPC)
    - EUB 3 – 2015: Experimental Platforms
- Call – Digital Security: Cybersecurity, Privacy and Trust
    - FCT-1-2015: Forensics topic 1: Tools and infrastructure for the fusion, exchange and analysis of big data including cyber-offenses generated data for forensic investigation.
    - FCT-4-2015: Forensics topic 4: Internet Forensics to combat organized crime.
    - DS-1-2014: Privacy
    - DS-2-2014: Access Control
    - DS-6-2014: Risk management and assurance models
    - DS-3-2015: The role of ICT in Critical Infrastructure Protection
    - DS-4-2015: Secure Information Sharing
    - DS-5-2015: Trust eServices.

As mentioned earlier, it wasn't really possible to carry out a similar mapping of the BIC ***Tactical Recommendation*** to H2020 since the first call of H2020 does not include International cooperation actions. We will discuss a solution for this with the relevant government bodies, including the Commission, to accelerate the Tactical Recommendations take-up as suggested here in D3.2 and in the Deliverable D2.5, Final report of the working groups, in which further suggestions on how the BIC IAG and EWGs should continue.

[13] http://ec.europa.eu/research/participants/portal/doc/call/h2020/common/1587758-05i._ict_wp_2014-2015_en.pdf

[14] http://ec.europa.eu/research/participants/data/ref/h2020/wp/2014_2015/main/h2020-wp1415-security_en.pdf

6.0 Conclusions

The development of modalities for international cooperation in cyber security is the cornerstone of achieving the global security of the digital ecosystem: cyber defence can never be effective without having an international dimension. Cyber threat with its inherent international dimension involves local, regional and global issues. International cooperation allows everyone to describe their own differences in terms of culture, the nature of threats and legislation, and to share diverse ideas, thus creating a common platform that unites the various continents. The diversity of approaches may be geographic (earthquakes in Japan prioritising the need to develop robust infrastructures) or cultural (language diversity in Europe leading to different linguistic approaches). A sustained dialogue and consolidation at the international level are important to validate the interoperability issues.

The need for an international global extension and for cross-discipline collaboration has become more urgent during the last decade. A long term strategy for international cooperation should include a move to a more sustainable methodology for multi-lateral cooperation models, involving all countries. Resilience of cyberspace is indispensable for assuring business continuity, the proper functioning of governments and law enforcement agencies and gaining the trust of citizens in these services. Field testing of the cyber infrastructure, contingency plans for emergencies, training of the stakeholders for unexpected situations, disaster-recovery including secure recovery of critical information, all require thorough consideration of the technological landscape as well as social and organisational behaviours.

This ecosystem requires a long-term vision and a regulation adapted to the challenges resulting from 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 legislative framework. International cooperation makes possible a dialogue and a commonality to express, in computer terms, the practical implementation of human values in the digital field, such as the questions of observing the behaviour of individuals, sovereignty over their personal data and the monitoring of the internet. Technological support for achieving digital credibility will be the cornerstone in making the digital ecosystem viable. Technological support is indispensable for translating governance policies and business rules into the practices and operations that result from new complexities and scalability.

To conclude, while the requirement for comprehensive international cooperation involving research, industry and government is established, it is imperative that a globally acceptable and sustainable mechanism is developed that ensures the practical implementation of this philosophy of international cooperation. Towards this end, the adaptation of the strategic and tactical recommendations (SRs & TRs) of this BIC project report is extremely significant. Particularly the recommendations on creation and sustenance of the empowered in-country Extended Work Groups(EWGs) and a centralised International Advisory Group (IAG) will be vital in bringing about the Trust worthy ICT and a sustainable ecosystem for effective cyber security against an extremely dynamic and evolving environment of cyber threats.

In the current H2020 calls, it is not clear whether this global vision and this global scale is taken into account, as many of the International actions are relegated to the second call for proposals. It is, therefore, essential for Europe to create, at the earliest, calls for proposals in the framework of international cooperation, to reconcile points of view, on a continental scale.

Research priorities

Six priority topics have been identified as a list of potential topics by the EU and Brazil, India, South Africa researchers for mutually beneficial cooperation in the area of trust and security. The 6 topics are:

1. Cybersecurity;
2. Trust and Privacy;
3. Mobile security, Social media and Cloud security;
4. Security of Applications and data protection;
5. Identity management, accountability frameworks;
6. Future Internet security.

The long-term **Strategic Recommendations** (H2020 and 2015-2025) for international cooperation in the field of Trustworthy ICT research and technological development are the following:

1. There is a need for new global approaches, meta-models and methodologies;
2. Global cybersecurity should be accepted as a moving landscape of attacks, surveillance and failures;
3. International cooperation research is an essential H2020 requirement;
4. The international community must agree on grand principles;
5. There must be a shift in emphasis from the tactical bi-lateral collaborations to a strategic multi-lateral approach;
6. There is a need to keep an international open-ness in specifications of services and standardisation;
7. There is a need for an international mobility model approach;
8. There is a need for an international approach dealing with the massive abstraction of software and data (e.g. resilience of virtualisation);
9. An international cooperation is needed to deal with the fragility of interconnections;
10. We need an international approach to steer the evolution and strengthening of the digital ecosystem in terms of network security governance and surveillance.

The more concrete **Tactical Recommendations** to be undertaken in the nearer term are:

1. The work of the BIC project, or its structural components (IAG, WGs) should be continued, and expanded to other countries, in the long term;
2. The EU and BIC countries should formally recognise the Extended Working Groups as the nodal in-country agency/body to be called upon for discussions regarding future H2020 (and beyond) international cooperation activities;
3. The EWG should establish and formalise their terms of references / objectives in synchronisation with one another and get these ratified by their respective Programme Management / Governments.

7 - References

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

[2] BIC survey on priority topics http://www.bic-trust.eu/priorities-survey/

[3] Observer Research Foundation (ORF) / Federation of India Chambers of Commerce and Industry (FICCI) Cy Fy 2013 conference, 14-15th October, 2013, New Delhi, India, http://orfonline.org/cms/export/orfonline/img/cyfyn/index.html

[4] Oberserver Research Monitor, Volume II Issue 1 January, 2014, http://orfonline.org/cms/export/orfonline/html/cyber/4-1.pdf

[5] DG CONNECT Trust and Security Unit H.4. http://ec.europa.eu/digital-agenda/about-trust-and-security; Unit H.4. Twitter feet: https://twitter.com/EU_TrustSec

[6] ICT EU-Brazil Coordinated call 1. http://ec.europa.eu/research/participants/portal/desktop/en/opportunities/fp7/calls/fp7-ict-2013-eu-brazil.html

[7] ICT EU-Brazil Coordinated call 2. http://ec.europa.eu/research/participants/portal/desktop/en/opportunities/fp7/calls/fp7-ict-2013-eu-brazil.html

[8] Brazil Extended Working Group Launch Workshop, October, 2013, http://www.bic-trust.eu/events/bic-brazil-ewg-launch-meeting/

[9] HORIZON 2020, WORK PROGRAMME 2014 – 2015, 5. Leadership in enabling and industrial technologies i. Information and Communication Technologies, http://ec.europa.eu/research/participants/portal/doc/call/h2020/common/1587758-05i._ict_wp_2014-2015_en.pdf pp. 92-94.

[10] 4th Euro-Africa Cooperation Forum on ICT Research 2011 http://euroafrica-ict.org/events/archives-cooperation-forums/2011-cooperation-forum/

[11] 5th Euro-Africa Cooperation Forum on ICT Research 2012 http://euroafrica-ict.org/2012-africa-eu-cooperation-forum-on-ict/

[12] 6th Euro-Africa Cooperation Forum on ICT Research 2013 http://euroafrica-ict.org/events/cooperation-forums/2013-africa-eu-cooperation-forum-on-ict/

[13] Information Security for South Africa Conference (ISSA) 2011 http://icsa.cs.up.ac.za/issa/2011/

[14] BIC EWG meeting, Addis Ababa, Dec. 2013, http://www.bic-trust.eu/2013/12/02/bic-south-africa-ewg-dec2013/

[15] BIC India Workshop, Dec. 2011, http://www.bic-trust.eu/files/2012/01/BIC_India.pdf

[16] BIC India EWG launch workshop, May, 2013 and follow up workshop, Oct., 2013, http://www.bic-trust.eu/files/2013/07/BIC-DeitY-EWG-report-final.pdf and http://www.bic-trust.eu/files/2013/10/BIC-DeitY-EWG-Oct-13-report.pdf

[17] Feb. 2013, UN Comprehensive Study on CyberCrime http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

[18] ENISA Guidebook on National Cyber Security Strategies Report http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-an-implementation-guide/at_download/fullReport

[19] BIC Workhop, June 2013, http://www.bic-trust.eu/files/2013/08/TAFC2013-Workshop-Report.pdf NSF programmes summary on pg. 6.

[20] Network Information Security Platform kick off WG meeting, Sept. 2013, http://ec.europa.eu/digital-agenda/en/news/nis-platform-kick-meeting-working-groups

[21] NIS Platform plenary and second WG 3 meeting, Dec. 2013, http://ec.europa.eu/digital-agenda/en/news/second-meeting-network-and-information-security-nis-platform-plenary

Annex 1. EU – International priority research areas in Trustworthy ICT for BIC countries

A1.1 Brazil – EU priority research areas in Trustworthy ICT[15]

The following section summarises key research themes in Trustworthy ICT that have been discussed for Brazil – EU collaboration within the BIC Project.

1. Research involving cybersecurity

Background: on November 30, 2012, Brazilian President Dilma Rousseff enacted two new laws that change the Penal Code and introduce new crimes related to the Internet and electronic communications.

The first law (No. 12.735) provides for granting judicial police departments to organize, in accordance with regulations, new organs and specialized teams to fight against criminal activities involving computer networks, communication devices and systems information.

The second law (No. 12,737) criminalizes the use of data obtained from debit and credit without the permission of the owner. This practice, considered as the falsification of a private document, is now punishable on conviction of one to five years in prison and a fine.

In 2012, Brazil adopted the White Paper to Guide Future Defense Priorities. The document foresees the creation of a full-fledged Brazilian Center for Cyberdefense (CDCiber) by 2015. The White Paper stresses that "the protection of cyberspace covers a wide range of areas such as training, intelligence, scientific research, doctrine, preparation and operational employment and personnel management. It also comprises protecting their own assets and the ability to networked operations [8].

Research Challenges of Mutual Benefit: Within BIC, the following activities have been identified where Brazil – EU collaboration could provide mutual benefits related to cybersecurity:

- **Physical and cyber worlds**: With the emergence of wireless network sensors, IoT, and robots, the interaction of physical and cyber worlds brings in human social aspects into the digital world. It is therefore necessary to first understand the cultural framework of all the populations and all stakeholders.
- **Regulations**: Appropriate regulations are needed in order to coordinate efforts from different stakeholders to try to develop a roadmap of cybersecurity practices that will be sharpened in the future in order to ensure a leading role of Europe and Brazil together in the digital ecosystem.
- **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). Measures should

[15] These topics are not meant to be exhaustive; however, they derive from the activities within the Building International Cooperation (BIC) for Trustworthy ICT FP7 Project http://www.bic-trust.eu/ . Please see the project impact section http://www.bic-trust.eu/impact/ for more detailed reading materials on these topics.

also allow the data exchange between EU and Brazil to analyse cybercrime and share experiences.

- **Threats, attackers and hacktivists**: 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 manner. Threats landscape is constantly changing. To collectively fight against cyber-threats more effectively, a coordinated response between EU and Brazil is required to understand the emerging threats and identify solutions and create a roadmap of actionable activity schemes.
- **E-governance, information sharing, sharing of best practices**, surveillance and analysis, joint exercises in cybersecurity and training, and joint research activities to foster collaboration between international and national, agencies as well as the private sector, are required. Multi-polar cybersecurity governance is needed for the Brazil context.
- **Cybercrime** (virus in email, botnets, Trojan in webpage, fraud in ecommerce, e-robbery in e-banking transaction, identity theft in credit card payment, …);
- **Cyber-terrorism**: 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 has become a tangible threat to the reliability of critical infrastructures of countries that are more or less related to digital infrastructures. However, the term of cyber-terrorism is differently understood in various countries. The international community has not yet been able to agree on the vocabulary and basic concepts. EU-Brazil 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.
- **CERT**s (Computer Emergency Response Team) recognised as premier references: Initiatives for the creation of CERTs or digital security task forces at national, continental, and international levels with clearer distinction of the roles of different actors. 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. An important element of the EU cybersecurity strategy will be significant efforts to harmonise the cybersecurity capabilities of European Member States via a well-functioning national-level (CERT).
- **Cyber forensics** for tracking attackers and enforcement purposes, protection against the social network of hacker groups, post-incident investigations are very important to analyse the perpetrators of digital crimes and to prosecute them for their activities. New frameworks and modalities are needed to meet the requirements of performing digital investigations of cyber world. These new techniques need to consider the peculiar characteristics of societal diversity and cultural backgrounds besides globalisation of criminals and their targets.
- Advanced and specialised **courses** to create a culture of security, privacy and trust; cooperation with EU must be enhanced in this area in order to create better awareness about cybersecurity.
- **Protection against malware**: the establishment of joint action teams of experts from the EU and Brazil can create more effective clout/momentum to identify and overcome these challenges collectively rather than individually. Figure A6 shows the

situation in Brazil in relation to malware and potentially unwanted software categories from a study carried out in 2012.

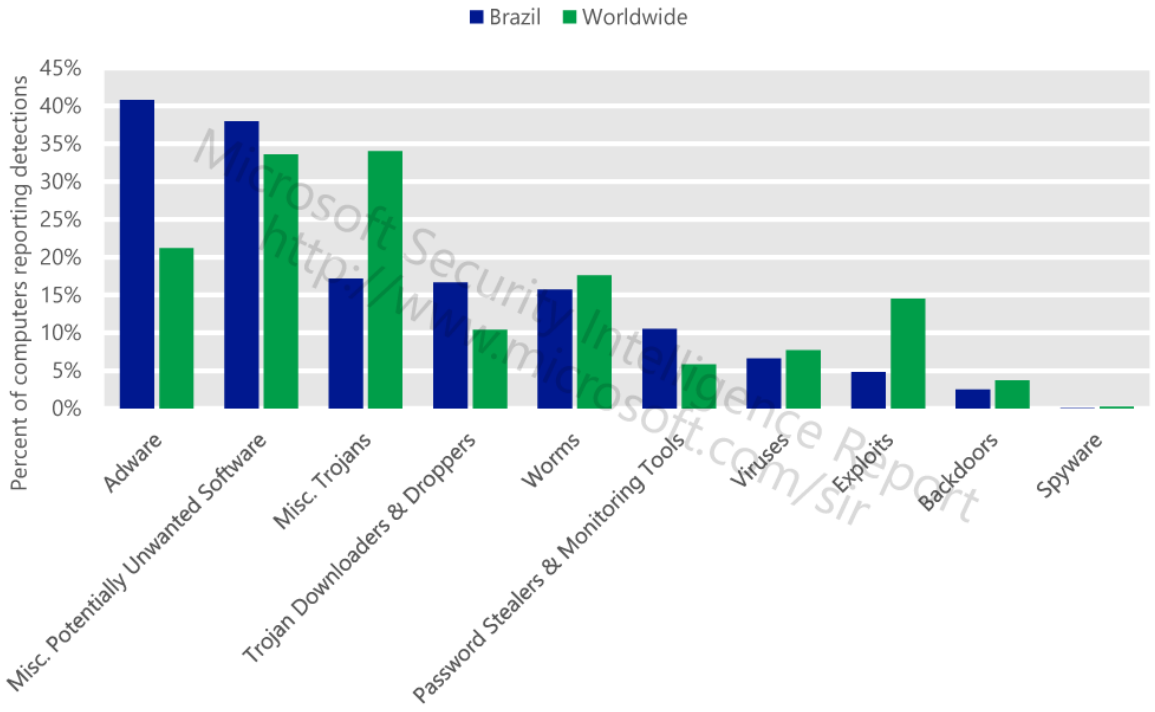

Figure A6. Malware and potentially unwanted software categories in Brazil in 2012, by percentage of computers reporting detections (Microsoft Security Intelligence Report))

2. Future Internet (FI) Data and Information provenance

Background: 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 ultimate source (provenance) is typically lost in the process of copying, or transcribing, or transforming databases. Provenance is essential to data integrity, currency and reliability and is a topic of importance being studied in Brazil. Future Internet data and information provenance (trusted source), especially during times of disaster and large scale events, is a topic that has been highlighted during the BIC interactions from the start 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.

Research challenges of mutual benefit: Within BIC, the following activities that Brazil – EU collaboration could provide mutual benefits related to FI Data and Information provenance have been identified:

- **Scientific Domains**: Scientists deal with greater heterogeneity in data and metadata- Trust, quality, and copyright of data are significant when using third-party data- E-Science - Business Domains.
- **Virtual organizations**: workflows, warehouse environments, where lineage information is used to trace the data in the warehouse view back to the source from which it was generated.
- **Governmental Domains**: In Brazil, within the social inclusion policies, this is a very important issue. E.g. Voting system, taxing system.
- **Data Quality**: use of lineage to estimate data quality and data reliability based on the source data and transformations.
- **Audit Trail**: tracing of the audit trail of data, determine resource usage and errors in data generation.
- **Replication Recipes**: allow repetition of data derivation, help maintain its currency and re-do replication
- **Attribution**: the pedigree can establish the copyright and ownership of data, help to determine liability in case of erroneous data.
- **Informational lineage**: use of lineage to query metadata for data discovery.
- **Applications**: Some examples of the applications in the different domains are such as collecting and modelling provenance from heterogeneous applications and data sources, integrating distributed and incomplete provenance information to compose complete provenance models and the effective management and querying of distributed, semantic provenance repositories for different applications.
- **Standardization**: There are a number of recommended actions within the scope of research cooperation projects are standardization of provenance models, services, and representations, provenance management architectures and techniques, analytic provenance and the relationship between provenance and visualization, provenance and the semantic web, human interpretation of provenance security and privacy implications of provenance, provenance and social media and provenance implications for trust.

3. Future Internet (FI) Data and Information privacy

Background: Within the Future Internet, which will contain a large mix of 'smart' technologies, including Internet of Things, mobile devices, cloud computing & cloud Storage, amongst others, data and information privacy is a major challenge associated with 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.

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 privacy, governance and liability are critical. Trust, Security, Privacy Compliance Management and Information Security Assurance are key international policy elements that need to be developed between Brazil and the EU. They need to be detailed from a multi-national and multi-cultural viewpoint.

There are complementary skills in Europe and Brazil on these research topics and they can be leveraged well together on this topic.

Research challenges of mutual benefit: Within BIC, the following activities that Brazil – EU collaboration could provide mutual benefits related to FI Data and Information privacy have been identified:

- **Smart technologies 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 technologies and privacy**: 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 on-going 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.

These latter research topics were the subject of a recent Brazil – European Union Dialogue conference on Digital Economy, Cloud computing, Security, Privacy and Data protection (see annex 3) held in Brasília, Brazil on 12th March 2013,

The BIC project was invited by Brasscom via an IAG member at University of Brasília (UnB) to attend the full day event in Brasília with prominent government, industry and researchers from Brazil and the EU Commission presenting areas for cooperation including Digital economy, cloud computing, privacy and data protection.

A significant amount of networking was possible during the event and the BIC project was described to the delegates from both CNPQ and the European Commission delegation and they said they would lend support to the setting up of BIC External Working Groups into the future.

4. Digital Identity Management

Figure A7. National Identity card in Brazil

Background: This research activity has been especially promoted by the Brazilian research community including RNP (Rede Nacional de Ensino e Pesquisa), PUC Rio amongst others, as an important area of potential cooperation between EU and Brazil.

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 Wi-Fi networks. This was being demonstrated 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.

Research challenges of mutual benefit: Within BIC, the following activities that Brazil – EU collaboration could provide mutual benefits related to Cloud security have been identified:

- **Authentication and Authorization**: In the areas 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. The different nature of business environments and political landscapes between EU and Brazil require a fresh look into the risks of using delocalised processing and storage of data and information. Generally businesses are advised to use Cloud technologies for the low risks processes. However, we need to work on different risks and perception of risks to see how harmonised risk models can be developed.

- **Digital Certification**: Digital Certification is a tool that enables cybercitizens to do safety electronic transactions, such as sign agreements and get access to restricted information, among others. It's also a fundamental tool in the businesses dematerialization process actually in course not only in Brazil but over the world. Within their ICP-Brazil: The National Digital Certification System, Brazil already has a relevant set of digital certification ready applications, mainly in bank industry, in the judiciary, in electronic invoices, in private and public health system and in a myriad of e-government systems. All of these nationwide applications have proven in practice the interoperability and security of ICP-Brazil and its Certification Authorities. In addition to identifying the Brazilian citizens in the web, the ICP-Brazil digital certificates offer identification services based on the current legislation and legal validity to the acts done with their use. Digital certification is a tool that enables application like e-commerce, e-sign of agreements, e-bank transactions, e-government services, among others. These are virtual transaction, i.e. without the physical presence of individuals, but where personal unequivocal identification is a must despite the operations are done by Internet.

- **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.

5. Trust management models for emerging countries

Background: This research topic has been collectively identified by all three BIC countries for international cooperation with the EU. It concerns the development of trust models, mechanisms and architectures to support business ecosystems.

Research challenges of mutual benefit: Within BIC, the following activities that Brazil – EU collaboration could provide mutual benefits related to trust management have been identified:

- **Cultural frameworks**: Techno-socio business ecosystems require a comparative analysis of cultures. Trust is a social behaviour and therefore managing trust requires managing behaviours. These cultural and social controls need to be analysed and mapped with the other communities to establish trust among these communities.

- **Reputation models**: The reputation of individuals is determined on various parameters including but not limited to their social status, community affiliation. Developing reputation models for their online behaviour and harmonise them with their cultural understanding of reputation requires new holistic approach to develop new reputation models that can effectively work with their European counterparts.

- **Interaction with the broader society**: It is important to study a broader segment of society and test the prototype of the new trust models at mass scale because results will be better and more accurate with larger sample size. It is therefore important to include wider communities and social groups including urban and rural groups to study and analyse their peculiar stand on trust and reputation and how to use these beliefs in global business ecosystem.

A1.2 India – EU priority research areas in Trustworthy ICT[16]

The following section summarises key research themes in Trustworthy ICT that have been discussed and earmarked for India – EU collaboration within the BIC Project. This section was supplemented with addition comments from India researchers that attended the launch of the BIC India External Working Group (EWG) in May 2013 [9].

1. Research within cybersecurity

Background: India and the EU have both recently released their national cybersecurity strategies:

- 7th February, 2013. The EU Cybersecurity Strategy of the European Union: *An Open, Safe and Secure Cyberspace*[17], was published.
- 9th May, 2013: India's National Cybersecurity Policy was approved by the Government of India[18];
- 2nd July, 2013. India's National Cybersecurity Policy[19] was formally notified.

The approaches of both EU and India towards cybersecurity policy have similar focus points:

a. ICT is a driver/engine for economic growth, innovation and prosperity;

b. Stress need for augmenting indigenous capabilities and focus on training;

c. Stress need for strategic partnerships, cooperation and collaborative efforts across all relevant stakeholders;

d. India has set up Joint Working Group (JWG) on cybersecurity to counter cyber attacks in economic and social infrastructure development;

e. The EU is in the process of setting up a Network Information Security (NIS) technology platform, whose objectives are to discuss standardisation needs and economic, legal and technological incentives that could be defined at EU, national or sectorial level. For the NIS platform, a Call for expression of interest was published on April 18, 2013 – see http://ec.europa.eu/information_society/newsroom/cf/itemdetail.cfm?item_id=10289. The output of the platform will feed into the Commission recommendations on cybersecurity, as well as the implementation of the risk management and incident reporting obligations under the proposed NIS Directive.

Research Challenges of Mutual Benefit: Within BIC, the following activities have been identified where India – EU collaboration could provide mutual benefits related to cybersecurity:

- 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

[16] These topics are not meant to be exhaustive; however, they derive from the activities within the Building International Cooperation (BIC) for Trustworthy ICT FP7 Project http://www.bic-trust.eu/ . Please see the project impact section http://www.bic-trust.eu/impact/ for more detailed reading materials on these topics.

[17] http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cybersecurity

[18] http://timesofindia.indiatimes.com/tech/tech-news/internet/Government-approves-National-Cybersecurity-Policy/articleshow/19965501.cms

[19] http://deity.gov.in/sites/upload_files/dit/files/National%20Cyber%20Security%20Policy%20(1)_0.pdf

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 cybersecurity 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. ***[A common minimum law or set of principles for trustworthy ICT need to be agreed by nations. These principles can further be built upon to arrive at Global Agreement codifying Cybersecurity Laws - Dr. Jaijit Bhattacharya, Director, Government Advisory, Hewlett Packard.]***
- 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 losing 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 more effectively, an organized response is requested to understand the emerging threats and identify solutions and create a roadmap of actionable global activities**. *[Today the government are rapidly IT enabling all its activities. It is collecting enormous information on individuals which is stored in various databases and shared across various organs of the government. Hacking into these databases will hurt immensely the concerned individuals. There is need to initiate international cooperation and multinational protocols are to be made to handle cyber threats and crimes as e-governance solutions are being extensively used to promote government programmes – Dr. N Vijayaditya, Ex CCA and DG, NIC, Govt. Of India]***
- E-governance, information sharing, sharing of best practices, joint exercises in cybersecurity and training, and joint research activities to foster collaboration between international and national, federal, state, and local agencies as well as the private sector have been promoted in BIC; ***[It is also essential for each country to work out security standards and make efforts to promote for their implementation. This would require committed international cooperation and joint work . Each country should essentially create process, both in software and hardware as most of the financial systems are being e-enabled. Additionally an integrated approach with the involvement of industry in the research, prototyping and testing can be undertaken. This will facilitate better monitoring and utilisation of the research - Dr. N Vijayaditya]***
- Cyber crime (virus in email, botnets, trojan in webpage, fraud in ecommerce transactions, e-robbery in e-banking transaction, identity theft in credit card payment etc;
- 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.

- CERTs recognised as premier references. For example, an important element of the EU cybersecurity strategy will be - significant efforts to harmonise the cybersecurity capabilities of European Member States via a well-functioning national-level Computer Emergency Response Team (CERT). The experiences from CERT-In could be a very meaningful contributor towards elaborating and achieving this objective.
- Cyber forensics for tracking attackers and enforcement purposes, protection against the social network of hacker groups, and establishing their Modus Operandi;
- Advanced and specialised courses to create a culture of security, privacy and trust;
- 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. The establishment of joint action teams of experts from the EU and India can create more effective clout/momentum to identify and overcome these challenges collectively rather than individually.

Figure A8 shows the situation in India in relation to malware and potentially unwanted software categories from a study carried out in 2012. ***[International Communication Systems rely on a diverse network of Telecom equipment. Any compromised equipment in such global systems can compromise the entire network. A robust international cybersecurity agreement is needed to identify and prevent such breaches. Collaboration among nations could also be to develop open source software for mutual benefit - Dr. Jaijit Bhattacharya]***

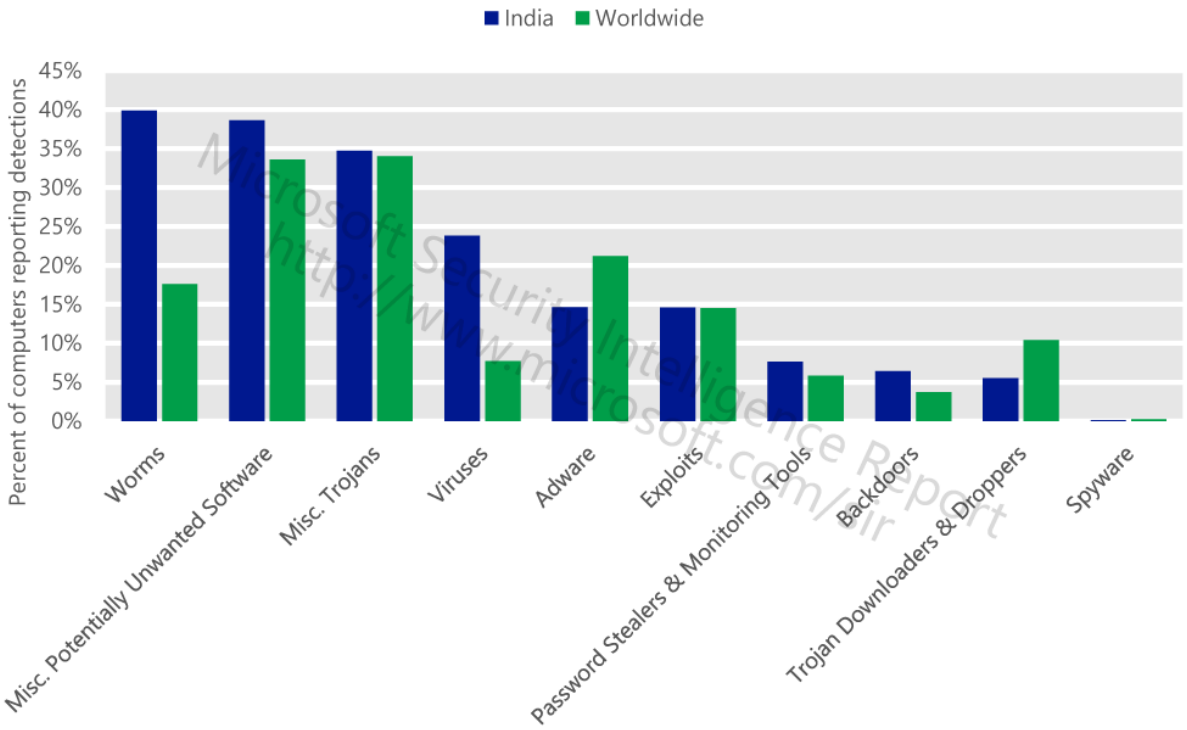

Figure A8. Malware and potentially unwanted software categories in India in 2012, by percentage of computers reporting detections (Microsoft Security Intelligence Report))

2. Mobile Security

Background: The extent and dimensions of the usage of mobile devices flooded with numerous applications has extended to practically all spheres of human life. These devices are now used for communication by voice, entertainment, social media, utility, information gathering, news, sports etc. in unimaginable proportions. With organizations increasingly looking toward mobile devices (e.g., iPhones, iPads, and Android smart devices) to deliver content and functionality to both their employees and their customer base and the people utilizing power of mobile applications more and more, the mobile devices are becoming the fastest growing consumer technology. However, most find it difficult to understand and evaluate the security concerns that surround mobile platforms.

The researchers involved in BIC from the EU and India (and indeed from the other involved countries like Brazil and South Africa) have repeated the need and urgency 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. This is especially important in India where the current approximate count of mobile users is nearly 700 million with 20-25% being GPRS users and 7% as smart phone users, which is growing at a rapid rate.

Research challenges of mutual benefit:

- 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.
- 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. The industry perspective has promoted the need for a dynamic security development from the developers' perspective that can move as quickly with the software developments taking place in the India marketplace to ensure a secure experience for their customers.
- Security that affects every day citizens:
    - Prevention of the Cloning Mobile SIM cards: Cost to an individual, whose SIM has been cloned, a breach of privacy, a significant terrorist implication, fall out on innocent people.
    - E-commerce security: Mobile Money transactions.
    - Application & Data Security: Applications like "Phone Data Backup" which back up the individual's phone data on cloud and assures user to keep it secure & protected. Similarly other mobile applications, which too deal with users' personal data e.g. Whats App, True Caller, etc.

3. Identity Management

Background: The trust in the emerging eServices in the areas of cloud computing, mobility, Internet of Things (IoTs), Future Internet, etc. essentially depends on the realisation of a highly interoperable techno-legal layer that enables privacy-respecting and trustworthy electronic identity services. There is significant work in both EU and India on Identity Management and implementation of one of these systems is in an advanced stage of rollout within India. There are associated Security, trust and privacy implications and consequent research challenges that can be addressed collectively between the countries. ***[Identity and authorisation are one of the major issues; Biometric based system are being proposed for identity and authentication. Such solutions need to be studied with respect to local features for facilitating faster and more accurate recognition. The algorithms need to be developed to accept these features. - Dr Vijayadita .]***

Research challenges of mutual benefit: The mutual cooperation can yield significant progress in the following fields:

- Effective engineering and technical solutions (e.g. PETs) to embed privacy by design and privacy by default (right to be forgotten) and into the design of ICT systems.
- Interoperable electronic and Internet-based identity schemes allowing federation and cross-border, cross-domain, cross-sector interactions.
- Privacy respecting identity management involving private and government third parties: identity/attribute providers, service composition… In particular, this requires international agreement on consistent metrics and assurance levels as well as basic understanding and acceptance of common fundamental principles[20] underlying different data protection legislations which may be universally applicable as a general framework (while recognising local specificities).
- More dependable ICT infrastructure articulated over mechanisms for accountability, liability, audit, compliance monitoring, enforcement… even across heterogeneous legal and trust domains.
- As a starting point, co-operation between India's Unique Identification (UID) project[21] and the EU's privacy protecting IDM research communities could look at ways to guarantee protection of the citizen's rights, security, privacy in the context of India's Unique Identification (UID) project:
- 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.

4. Trust management models for emerging countries

Background: This research topic has been collectively identified by all three BIC countries for international cooperation with the EU. It concerns the development of trust models, mechanisms and architectures to support business ecosystems. For these systems, it is important that trust management takes into account concepts relevant to the target context. An important identified focus of the research is the study of culture on trust. Cultural differences, while difficult to observe and measure, are obviously very important. Failure to appreciate and support them can lead to embarrassing blunders, and lower economic activity

[20] Principles of proportionality, purpose specification, lawfulness/fairness and rights of access, rectification, deletion, objection as stated in 2009 Madrid Declaration of Data Protection and Privacy Commissioners.

[21] Unique Identification Authority of India - http://uidai.gov.in/

and performance. ***[We need to work together to come out with a common acceptable definition and framework for trust. Need for creating a model contractual, competence and good will trust between and amongst Industry, Academia and Government stakeholders, so that the beneficiaries are indeed the citizens. -Mr Sanjay Bahl, Consultant, Info Security.]***

With specific regard to India, the evolving Government policy regarding the provision and delivery of services to the citizens[22] is increasingly Internet based and provides a context for research in "online trust models" to ensure the take-up of these services.

- The **National e-Authentication Framework (NeAF)[23]** is put forward to ensure secure online delivery of e-governance services across various platforms including mobile;
- India's **Mobile governance framework**[24] has emphasized the need for leveraging the high penetration of mobile platforms to facilitate citizen engagement.

Research challenges of mutual benefit: The mutual cooperation can yield significant progress in the following areas:

- The psychology of trust has deeper connotations and is influenced by the cultural backdrop of the people being investigated; therefore, a study of existing cultural frameworks to determine the most suitable to use;
- Extraction of relevant cultural behaviours and beliefs that are applicable to consumer trust and a study of trust models to identify the most applicable to use for business ecosystems in communities; and the enhancement of trust models with cultural norms;
- The implementation and evaluation of a prototype system to determine if the culturally adapted trust model can be used in rural communities.
- For ensuring adequate uptake for the mobile cloud applications, we need to package them with due sensitivity to the trust dynamics of the target consumers;
- Research in the construct of "Online trust" models as applicable to the adoption of these emerging mobile applications in Indian and International context. The common denominators and differences amongst the researched cultures would provide deep insights, while designing trust, security and privacy applications.

[22] The Indian Government THE ELECTRONIC DELIVERY OF SERVICES BILL, 16th November 2011: The Central Government, the State Government and public authorities will deliver all public services by electronic mode within five years of the commencement of this Act.

[23] National e-Authentication Framework (NeAF) (Draft National e-Authentication Framework (NeAF)) has been conceptualised by the Department of Information Technology, Indian Government, on 01 Sep 2011, in an endeavour to increase citizens' trust in the online environment and to enable the various government agencies to choose appropriate authentication mechanisms.

[24] Framework for Mobile Governance by Indian Government, Jan 2012. The m-Governance framework of Government of India aims to utilize the massive reach of mobile phones and harness the potential of mobile applications to enable easy and round-the-clock access to public services, especially in the rural areas. The framework aims to create unique infrastructure as well as application development ecosystem for m-Governance in the country.

5. Additional topics highlighted by India researchers

The following items were additional commentary provided by the Government of India and Researchers at the Launch workshop of the BIC India IAG [6]. These comments didn't exactly fit within the above four topics so are included here instead.

Dr. MP Gupta, Professor, & Chair-Information Systems & E-government, Department of Management Studies, IIT Delhi

Dr. Gupta graciously offered to provide IIT Delhi facilities and resources to augment BIC endeavours towards the following:

- Formalise India's Extended Working Group (EWG) of BIC;
- Write to scholars from other institutions to be part of EWG;
- To plan an International meeting or symposium of scholars during January 2014 covering BIC 's H2020 planning agenda; [*It was pointed out that while this symposium would be most welcomed, the BIC project officially concludes at the end of December 2013, unless a no cost extension was sought and granted to cover an additional period in time. The Coordinator, J. Clarke, said he would check with the other project partners and Commission on this possibility. It was also suggested that funding might be made available on the India side as well if sought early enough as long as the event is held in India.*]
- Draft of brochure for the activities and events.

Dr Vijatadita Ex CCA & DG NIC, Govt. Of India

Cybersecurity is not just limited to an individual. It extends to organisations and to governments. Its effects are felt at various levels. Cybersecurity is also not a static phenomena but a highly dynamic one. Hence there are no permanent solutions and continuous research is essential to update the policies, processes and solutions.

Today, the government are rapidly IT enabling all its activities. It is collecting enormous information on individuals which is stored in various databases and shared across various organs of the government. Hacking into these databases will hurt immensely the concerned individuals. In such an environment, cybersecurity systems have to be robust. We also need to create a process and procedure to compensate the individual in addition to punishing the culprit. Research is needed to create models for implementation of such policies. Identity and authorisation are one of the major issues, Biometric based system are being proposed for identity and authentication. Such solutions need to be studied with respect to local features for facilitating faster and more accurate recognition. The algorithms need to be developed to accept these features.

Privacy is another issue that needs to be attended to. In a nutshell, there are several technical, economical and legal issues that need intense research for formulating the policies and protocol across organisations and countries.

In India, there are number of research projects going on in cybersecurity at academic level, research organisation and private institutions level. Some sort of coordinated consolidation approach is needed amongst all these researches for achieving the best possible results. This approach and associated actions have to be initiated at national level. These major problems need to be broken up into smaller projects which are then selectively assigned to different research and academic institutions. By this process the present and the future issues that may arise along with various technological developments can be suitably addressed. Additionally an integrated approach with the involvement of industry in the research, prototyping and testing can be undertaken. This will facilitate better monitoring and utilisation of the research.

It is also essential for each country to work out security standards and make efforts to promote for their implementation. This would require committed international cooperation and joint work .Each country should essentially create process, both in software and hardware as most of the financial systems are being e-enabled.

There is need to initiate international cooperation and multinational protocols are to be made to handle cyber threats and crimes. E-governance solutions are being extensively used to promote government programmes. In India, providing “Adhar” cards as a most important basis of individual identity for all its citizens is in progress. “Adhar” number is now being extensively integrated with financial and other government activities. Security issue related to this needs research on storing and access algorithms. In addition to finding solutions for preventing cyber threats, there is also an urgent need to find solutions and protocol for fast recovery.

There is a need to do much work to create trusted environment. We are looking at a scenario where all transactions will be done electronically. This would require all users to be reasonably educated in handling technology driven devices and systems whereas today a majority are just layman users. Secondly need to develop a standard protocol that could be adopted by all countries. Towards achieving this, there is need for coordinated international cooperation and integrated efforts.

Finally, each country need to create a structure where all cybersecurity aspects are looked into and make a clear cut well coordinate plan to prevent/protect its cyber properties.

Dr. Jaijit Bhattacharya, Director, Government Advisory, Hewlett Packard

1. Cyber warfare and cyber weapons are no less dangerous than conventional weapons. There is a need for a Global Treaty banning use and deployment of cyber-weapons by nation states. Escalation of cyber-warfare and race to build cyber-weapons could be disastrous to rival nations.
2. A common minimum law or set of principles for trustworthy ICT need to be agreed by nations. These principles can further be built upon to arrive at Global Agreement codifying Cybersecurity Laws.
3. Social Warfare such as inciting violence or abuse targeted against a particular community needs to be prevented. Any international co-operation treaty should be oriented towards preventing social warfare. Countries like India with diverse communities are especially vulnerable to such attacks
4. International Communication Systems rely on a diverse network of Telecom equipment. Any compromised equipment in such global systems can compromise the entire network. A robust international cybersecurity agreement is needed to identify and prevent such breaches.
5. Collaboration among nations could also be to develop open source software for mutual benefit.
6. There is a need to put in place a fall-back option in the event of a global internet blackout. A worst-case scenario should be worked out with back-up communication processes for the days following an internet catastrophe.
7. Building International trust and co-operation assumes increased significance in the issue of Internet Governance.
8. BIC should incorporate some tangible outputs in its Agenda. One of such examples could be building an international database of IMEI codes of mobile phones. This could be used to track unlawful criminal activity.

Mr. Sanjay Bahl, Sanjay Bahl, Consultant, Info Security

1. Need to come out with a common acceptable definition and framework for trust.
2. Need for creating a model contractual, competence and good will trust between and amongst Industry, Academia and Government, so that the beneficiaries are the citizens.
3. Need for inculcating information security and privacy culture and behaviour among users through a comprehensive and sustainable national awareness program by collaboration and innovation.
4. Study vulnerabilities in a sample Critical Information Infrastructure. This could be an opportunity to – provide a trust and reputation framework / model derived from statistical models for pattern analysis of threats detected in terms of
    a. Targets
    b. Signatures
    c. Attack vectors including vulnerabilities exploited
    d. Remediation / work-arounds suggested by vendors
5. Based on the above develop a trust and reputation model for each ICT product and also for each vendor for their appropriate future participation in cyber space and digital economy.
6. Develop scenario and model based policy frameworks to highlight potential gaps and understanding in existing policies.
7. Understanding the linkages between Security Governance and Security Quality along with their impact.

A1.3 South Africa – EU priority research areas in Trustworthy ICT[25]

The following section summarises key research themes in Trustworthy ICT for South Africa– EU collaboration within the BIC Project.

1. Research in cybersecurity

Background: The African 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. And now with the fast pace of increased broadband Internet penetration in Africa, there are apprehensions of whether Africa could become the home of the world's largest botnet or an unbridled cybersecurity pandemic. International, collaborative research can address these challenges by looking at a variety of approaches that require innovative implementation.

South Africa has released in May 2011 their national cybersecurity strategies[26]. In South Africa, the focus on cybersecurity is especially prominent since many geographical regions are incorporated into the global village in an attempt to bridge the digital divide. cybersecurity in South Africa especially includes a strong push on cyber-crime prevention and cyber forensics.

Research challenges of mutual benefit: Within BIC, the following activities that South Africa – EU collaboration could provide mutual benefits related to cybersecurity have been identified:

- **Physical and cyber worlds**: The interface of physical and cyber worlds brings in human social aspects into the cyber world. It is therefore necessary to first understand the cultural framework of the collectivist African society where people emphasize interpersonal relationships; and where loyalty is obtained by protecting the group members for life. Individuals see themselves as subordinate to a social collective such as a state, a nation, a race, or a social class. They prefer group harmony and consensus to individual achievement.

- **Regulations**: Appropriate regulations are needed in order to coordinate efforts from different stakeholders to try to develop a roadmap of cybersecurity practices that will be sharpened in the future in order to ensure a leading role of Europe and South Africa together in the global cybersecurity.

- **International Data Exchange for cybersecurity**: Sharing of information with the stakeholders of the cyberspace is becoming a milestone in ensuring cybersecurity. An increasing number of regulators are therefore developing new rules for enforcing data

[25] These topics are not meant to be exhaustive; however, they derive from the activities within the Building International Cooperation (BIC) for Trustworthy ICT FP7 Project http://www.bic-trust.eu/ . Please see the project impact section http://www.bic-trust.eu/impact/ for more detailed reading materials on these topics.

[26] "Implementation of a cybersecurity Policy in South Africa: Reflection on Progress and the Way Forward",Marthie Grobler, Joey Jansen van Vuuren, Louise Leenen (http://link.springer.com/chapter/10.1007%2F978-3-642-33332-3_20)

sharing (e.g. data breach notification by ENISA). Measures should also allow the data exchange between EU and South Africa to analyse cybercrime and share experiences.

- **Threats, attackers, hackers**: South Africa's information security market is seeing a surge in activity as local companies struggle to come to grips with the challenges of consumerisation of IT, the advent of new information privacy laws and regulations, and the changing nature of the threats they face from malware and hackers. Figure A9 shows the situation in South Africa in relation to malware and potentially unwanted software categories from a study carried out in 2012. Threats landscape is constantly changing with the cat and mouse game between security designers and attackers and hackers. To collectively fight against cyber-threats a coordinated response between EU and South Africa is required to understand the emerging threats and identify solutions and create a roadmap of actionable activity schemes.

- **E-governance, sharing of best practices**: E-governance, information sharing, surveillance and analysis is required to foster collaboration among state and agencies as well as the private sector. Multi-polar cybersecurity governance is needed for South African context due to their heterogeneous social composition.

- **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 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.

- **Cyber-terrorism**: Cyber-terrorism has become a tangible threat to the reliability of critical infrastructures of countries that are more or less related to digital infrastructures. However, the terms of cybercrime and cyber-terrorism are themselves differently understood in different countries. The international community has not yet been able to agree on the vocabulary and basic concepts. EU-South Africa 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.

- **CERTs**: Initiatives for the creation of CERTs or digital security task forces at national, continental, and international levels with clearer distinction of the roles of different actors. 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.

- **Cyber forensics**: Post-incident investigations are very important to analyse the perpetrators of digital crimes and to prosecute them for their activities. New frameworks and modalities are needed to meet the requirements of performing digital investigations of cyber world. These new techniques need to consider the peculiar characteristics of societal diversity and cultural backgrounds besides globalisation of criminals and their targets.

- **Advanced and specialised courses to create a culture of security, privacy and trust**: 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. Cooperation with EU must be enhanced in this area in order to create better awareness about cybersecurity.

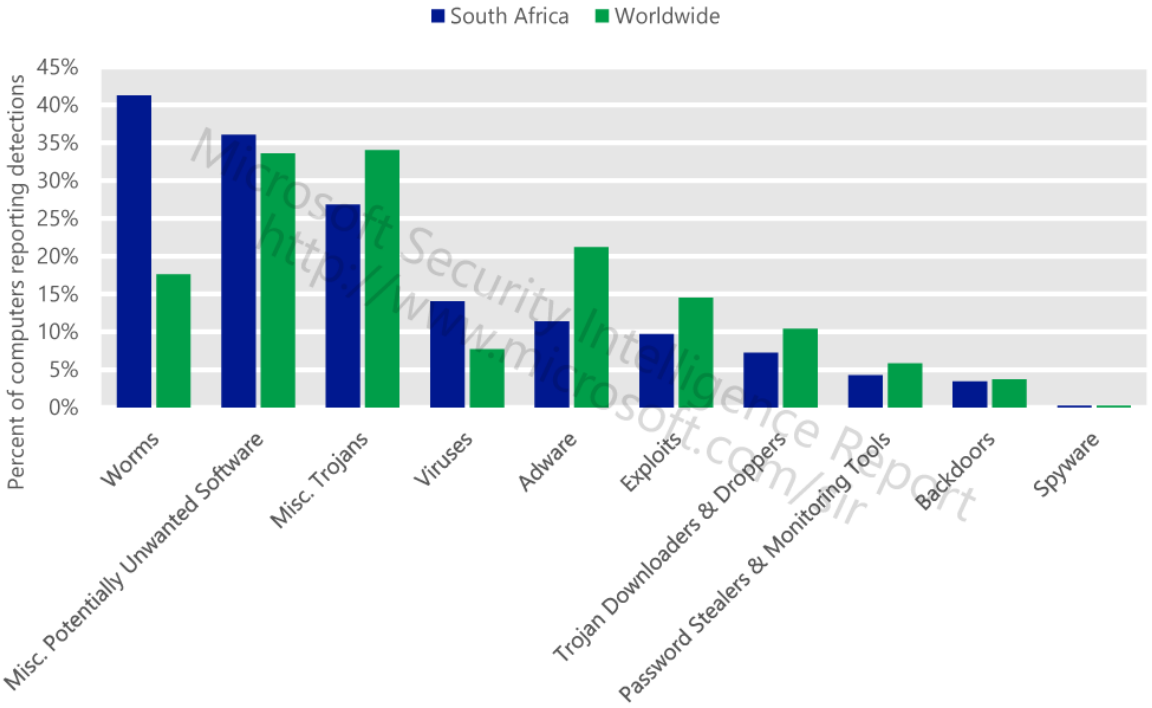

Figure A9. Malware and potentially unwanted software categories in South Africa in 2012, by percentage of computers reporting detections (Microsoft Security Intelligence Report))

2. Mobile Security

Background: The ever increasing trend of using smart and mobile devices across the global business and consumer markets can equally be observed in South Africa that has a comparatively well-established communications infrastructure in the African continent. Newer business models and the compliance requirements for the personal data protection brings the mobile security in the forefront of the challenges faced by the South African society in general and businesses notably services providers in particular. With tablets and smartphones accounting for a growing proportion of network and internet traffic, these devices are becoming an attractive target for malware authors and hackers. According to Symantec, mobile vulnerabilities have increased by 93% in 2011, with a strong rise in threats targeting the Android operating system.

Research challenges of mutual benefit: Within BIC, the following activities that South Africa – EU collaboration could provide mutual benefits related to mobile security have been identified:

Device security: Physical security of the mobile devices is the weakest link in the mobile security chain. Best practises including user awareness for the physical protection of these devices in the context of South Africa needs to be developed. This initiative should be complemented by the technical solutions to remotely erase the entire data of the stolen devices.

Societal issues: It is very important for EU to understand cultural issues and community based approaches towards privacy, information sharing and location-based services in the context of South Africa. Likewise the South Africans need to understand the European standards for these areas so as to develop convergence models for these areas.

Data protection jurisdictions: Application of data protection is not limited to the mobile devices as they use some applications, backend servers, and networks for synchronisation. Moreover M2M connections often bypass monitoring and control solutions and are difficult to trace back. It is therefore very important to provide further details of the data protection jurisdictions to avoid any grey areas for the breaches to occur.

Regulations for Apps: Local app stores of open mobile systems are like public market square where anyone can sell anything. Viruses and other infected apps and software codes can be transmitted across the world from these local app stores. It is therefore quite crucial to ensure that some minimum security vetting standards are put in practise for these merchants.

Cooperation of stakeholders: Network operators and manufacturers of mobile services and products should cooperate to develop guidelines for the proactive installation of security patches; timely sharing of vulnerabilities and joint efforts to quickly fix them. EU and South African government can facilitate such cooperation by encouraging them to work together through some service incentives.

3. Cloud security (including security as a service)

Background: Cloud security is of paramount importance for the proper functioning of our near future digital economy as its scope is getting so wide that it is already seen as critical information infrastructure. Architectural shortcomings of Cloud deployments and trust issues still need to be overcome for the wider adoption of this technology by the businesses and governments. The growing use of mobile devices in enterprise workforces and the move to the cloud have opened up a new front in the arms race between enterprises and those that would attack their information and networks. It is not the network that is being attacked, but the application. The traditional concept of the enterprise network is obsolete, with the move to the cloud, the rise of mobility and a proliferation of peripherals and storage media. Organisations need to take a more multidimensional approach to security.

Research challenges of mutual benefit: Within BIC, the following activities that South Africa – EU collaboration could provide mutual benefits related to Cloud security have been identified:

Risk models: The different nature of business environments and political landscapes between EU and South Africa require a fresh look into the risks of using delocalised processing and storage of data and information. Generally businesses are advised to use Cloud technologies for the low risks processes. However, we need to work on different risks and perception of risks to see how harmonised risk models can be developed.

Uniforming uptake of Cloud solutions: According to the statistics given in a recent article[27] 'Cloud computing trend finds followers in SA' the uptake of Cloud solutions in South Africa is slower than Europe and USA. This difference will ultimately impact on the data security due to potential mismatch of security situations between in house IT security solutions and Cloud security solutions. It is therefore important that EU – South Africa collaboration aim to balance the pace of Cloud solutions uptake in South Africa so that security landscape also remains compatible with the European standards.

Security of data centres: The evolution of data centres remains key driver of Cloud computing ecosystem in South Africa[28]. This situation requires that EU – South Africa collaboration should explicitly include security of data centres. One possible dimension could be the enforcement of organisational security policies for these data centres through legislation and compliance requirements. However, all the other possible solutions should be pragmatically considered before selecting the best suitable option.

4. Trust management models for emerging countries

Background: This research topic has been collectively identified by all three BIC countries for international cooperation with the EU. It concerns the development of trust models, mechanisms and architectures to support business ecosystems.

Research challenges of mutual benefit: Within BIC, the following activities that South Africa – EU collaboration could provide mutual benefits related to trust management have been identified:

Cultural frameworks: Techno-socio business ecosystem requires a comparative analysis of individualistic culture (Europe) and Collectivistic culture (Africa). Trust is a social behaviour and therefore managing trust requires managing behaviours. These cultural and social controls need to be analysed and mapped with the other communities to establish trust among these communities.

Reputation models: The reputation of individuals in South Africa is determined on various parameters including but not limited to their social status, community affiliation. Developing reputation models for their online behaviour and harmonise them with their cultural understanding of reputation requires new holistic approach to develop new reputation models that can effectively work with their European counterparts.

Interaction with the broader society: It is important to study a broader segment of society and test the prototype of the new trust models at mass scale because results will be better

[27] http://www.bdlive.co.za/business/technology/2013/05/15/cloud-computing-trend-finds-followers-in-sa

[28] http://www.slideshare.net/SamanthaJames_5/cloud-computing-in-south-africa-reality-or-fantasy

and more accurate with larger sample size. It is, therefore, important to include wider communities and social groups including urban and rural groups to study and analyse their peculiar stand on trust and reputation and how to use these beliefs in global business ecosystem. An example of one such collaboration could include work between the security communities and the undersea cable communities, as depicted in Figure A10.

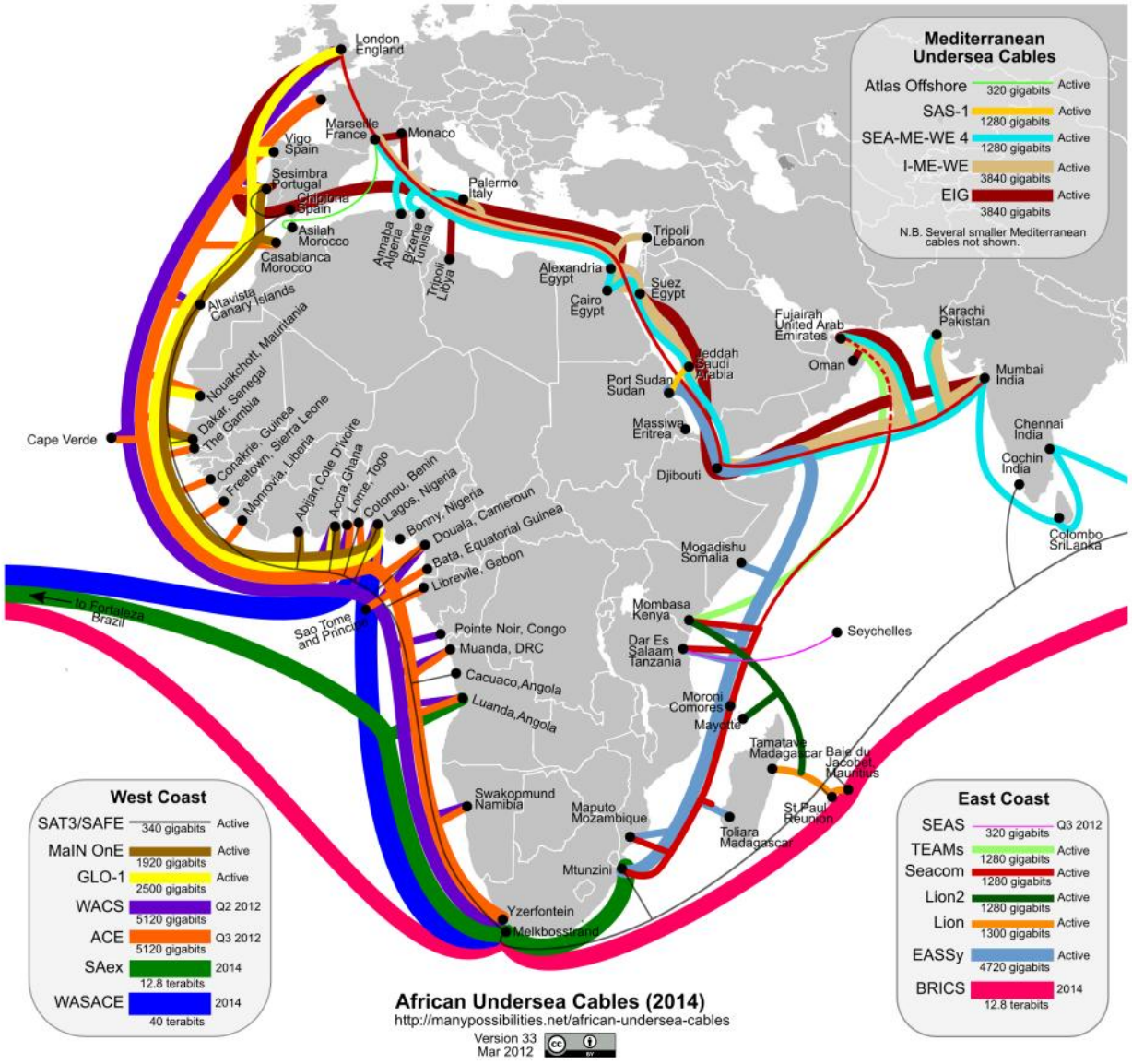

Figure A10. African Undersea Cables in Africa (2014)[29]

[29] http://www.flickr.com/photos/ssong/7087121729/sizes/o/in/photostream/

Annex 2. Mapping of priority research (Brazil, India, South Africa versus EU)

This annex develops a mapping exercise for international cooperation based upon the initial priorities as developed in the sections above. This mapping in Table A7 reveals foresee-able themes and topics for both bi-lateral and multi-lateral co-operations between the EU and BIC countries.

Brazil	India	South Africa	EU
Main issues and general approach for ICT trust and security			
The major concerns are cybersecurity, identity management, the Future internet security, trust management.	The main India issue, after cybersecurity, is mobile security.	The main south African issue is cybersecurity, including frauds and identity theft.	The main EU concern is citizen's privacy. The other issues are essentially cloud computing security and identity theft due to frauds. The network neutrality, the internet surveillance are also a concern.
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 the in-depth concepts 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
Cybersecurity : resilience of infrastructures, physical and logical infrastructure protection			
International cooperation in Cybersecurity: The need of a comprehensive research towards international Intelligence, Surveillance, and Reconnaissance (ISR) in the cyberspace domain is highlighted, 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. 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.	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. 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 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.	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 increasing complexity of IT systems and networks and expanding wireless connectivity present mounting security challenges that substantially increase their exposure to attack.	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.

Brazil	India	South Africa	EU
Trust and Privacy, data protection			
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 to provide adaptable and context-aware privacy protection mechanisms and tools for automatic customization and personalization of security services. 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. 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.	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.	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. 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, 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.	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' Balancing between the right to anonymity (privacy) and the societal imperative of making personal data available.

Brazil	India	South Africa	EU
Mobile security, Social media and Cloud security			
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. 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. Considering the mobile access the goal for 2014 is 60 million of broadband mobile access in the country.	The need and urgency 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. This is especially important in India where the current approximate count of mobile users is nearly 700 million with 20-25% being GPRS users and 7% as smart phone users, which is growing at a rapid rate. Security of Mobile telecom; building trust for Mobile transactions. Broadband coverage issues within India should be addressed before the cloud could become a major topic of coverage in trust and security	African entrepreneurs run profit ecosystems rather than business units. These ecosystems interact with other ecosystems in a culturally involved manner to ensure that the ecosystem will survive in the face of adversity. Social capital and social ties support these ecosystems and communities in large parts of Africa where members of communities pool resources together in an attempt to meet economic and social needs for both individual members and the general community. An identified need is the development of social computing technologies to support the growth and development of these ecosystems and communities to allow them to flourish.	Context-aware services and devices with localization systems will be offering attractive new functionality. People who travel and need access in mobile international environment, will use not only contents but likely other services such as on-line collaborations, 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. Cloud Computing & 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.

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	E-governance, information sharing, surveillance and analysis: to foster collaboration among federal, state, and local agencies as well as the private sector. 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 cybersecurity among students through ethical hacking contest. Multi-linguism issues in trust and security: language-independent information dissemination using NFC. Multilingual systems are a serious challenge in India.	Financial Infrastructure protection: Mobile phones can be used as a tool to intervene and act as a competitive force in the social, economical and political development. There is an opportunity to develop mobile social networking as a business in Africa, to growth the very small enterprises in these countries. This can ensure that communities can develop into positive, productive and outstanding environments by combining modern technology with the natural predisposition of people to culturally support each other.	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 secure and reliable manner.

Brazil	India	South Africa	EU
Identity management and Accountability Frameworks			
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, 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	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. Cryptographic protocols between Payment System Provider, Deposits, Payment and Authorization) for micro-payment is highly suited for India. The level of the Indian mathematics research is well recognized in applied mathematics: data mining and machine learning, formal approaches to security.	Identity and Authentication protocols are essential on Internet and in a mobile environment. 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 attacks on automobile computer systems. There are strong signs of this being organised cybercrime 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	The Identity Management approach in the EU is tightly coupled with privacy management as seen in the main projects dealing with IDM in the recent past, including PRIME, PRIMELIFE, and the currently running ABC4Trust project[30]. These European RTD projects are building their architectures based on privacy requirements collected within the European setting. However, they fully realise that privacy concerns differ in the international setting. It is, therefore, an open research question to be discussed how privacy relevant processing with and in countries like Brazil, India or South Africa can be handled within the European context. • How are concepts like proportionality, unlinkability, minimal disclosure etc. being perceived in other countries? • How other legal systems outside Europe can be affected by and have effects on Privacy-ABCs? • How to ensure an optimum balance between privacy and utility, taking into account local contextual

[30] https://abc4trust.eu/

security assurance of composed systems from an international data access perspective and EU compliant privacy laws. A survey of the activities undertaken by RNP (Rede Nacional de Ensino e Pesquisa) in the area of identity management as an area of potential cooperation between EU and Brazil. In the area of authentication and authorization, two independent groups led efforts related, respectively, to public key infrastructures and to federated authentication and authorization. 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.		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.	needs and preferences? The EU FP7 project A4Cloud[31] is addressing accountability approaches and mechanisms specifically for Cloud Computing. At the recent BIC workshop, a number of were identified as areas that would benefit from further international research: model contracts; binding corporate rules (BCRs); privacy management frameworks; technical standards; management standards; and privacy seals.

[31] http://www.a4cloud.eu/

Brazil	India	South Africa	EU
Future Internet Security			
Many challenges are introduced according to the necessary scenario transformation for Future Internet priority area in Brazil. 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. 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.	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.	"Could Africa become the home of the world's largest botnet or an unbridled cybersecurity 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.	Supporting and coordinating research across the continent and through international cooperation by prioritising the development of the 'Future Internet' through initiatives such as Future Internet Assembly (FIA) and FIRE. 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.

Table A7. Mapping of EU and BIC countries research agendas in ICT Trust and Security

Annex 3. Priority research and long term recommended actions for H2020

A - Priority research toward openness and expansion

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

We list below the issues of interoperability and harmonisation, taking into account the expansion of the ecosystem, diversity of cultures and usage and human aspects.

A - 1 - Conceptual models for governance, trust and data exchange

Research for fluidity of services, data and interactions in order to deploy a global ecosystem: design of models, metrics, tools and mechanisms.

Cyber-ethical and governance models

Models for global cyber-ethics *to maintain a smooth stream of social interactions and to work out the right balance between the rights, responsibilities, and obligations in the cyber realm and its real-world ramifications.*

Digital business models *to promote entrepreneurship in the digital world, evolutionary integration models for the ever-expanding and virtually limitless expansion of the digital world (Risk metrics for cloud usage for individuals, for businesses, and for administrations.)*

Suitable governance models *with necessary powers for the governors. Dependency metrics of digital ecosystem to protect the functioning of routine government and businesses.*

- ✓ **Cyber-ethics models**: development of models for global cyber-ethics to maintain a smooth stream of social interactions and to work out the right balance between the rights, responsibilities, and obligations in the cyber realm and its real-world ramifications. The recent past has seen diverse opinions about some high profile incidents (such as Wikileaks, Stuxnet) where totally different ethical approaches are taken by various segments of society.
- ✓ **Evolutionary integration models**: design of evolutionary integration model(s) for the ever-expanding and virtually limitless expansion of the digital world. 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 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.
- ✓ **Business Models**: development of digital business models to promote entrepreneurship in the digital world. 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 should provide better traceability of actions.
- ✓ **Digital governance model**: development of some suitable governance model with necessary powers for the governors. 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. The growth of the "added-value" of having such governance could inspire stakeholders to work under this protective umbrella.

✓ **Cloud regulation analysis**: 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.

Trust models

*Establishment of some **universal trust models**.*
*Harmonisation of national/continental **regulatory initiatives** at the global scale.*
*The flow of data and information across the geopolitical borders require some **global flow agreement** to facilitate the export control.*

✓ **Trust instrumentation**: establishment of some universal trust models where users will have suitable means to develop trust relationships based on communities. The universal trust model will need to address this situation where stakeholders will be able to establish trust without disclosing too many details that may then compromise their security and liberties.

Data exchange models

***Priority-management models** to facilitate the sharing of critical cyber data and information with peers at the global scale.*
*Mechanism for **responsibly sharing data** on cyber offenders'.*

✓ **Sharing data mechanisms**: mechanism for responsibly sharing data on cyber offenders' will help other stakeholders to be aware of the potential attackers in their surroundings. This approach must also deter the future cyber thieves from offenders' actions. It will also help policing the cyber territories.

✓ **Priority management**: establishment of 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 and structural.

A - 2 - Initiatives for education and research

Instructive and informative priorities for fluidity of usage, cooperation and awareness, preparation of public consultations, in order to enhance education and research: design of education, training and research programmes

The 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.

Education

Educational programmes *for general public to increase awareness and skills in secure use of the digital world.*

User awareness programmes *for different but overlapping groups of society, and cyber defence exercises for stakeholders involved in the digital ecosystem.*

- ✓ **User awareness programmes**: awareness raising programmes for general public should be developed to increase awareness and skills in secure use of the digital world.
- ✓ **User awareness programmes**: development of user awareness programmes 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 remains prevention.
- ✓ **Exercises**: 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.

Consultation

Public consultation for the ***perception of privacy*** *in the digital age to be helpful in outlining the data protection and digital behaviour monitoring minimisation requirements.*

Consultation on the concept of ***cyber deterrence*** *and its impact on the global security landscape.*

Early serious initiatives to launch the preparation and consequent adoption of legislation to facilitate the use of ***digital evidence*** *in courts of law.*

- ✓ **Privacy models**: public consultation for the perception of privacy in the digital age will be helpful in outlining the data protection and digital behaviour monitoring minimisation requirements. 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.

Global research framework

Europe should study, with fellow programme management and research communities, how to move to a more multi-lateral strategic level approach.

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

- ✓ **Research management harmonisation**: Europe should start, with fellow programme management and research communities world-wide engaged in international cooperation, to gain their insights on how to move to a more multi-lateral strategic level approach in the future.
- ✓ **Research framework**: strategic global research frameworks should be enabled in the H2020 funding mechanisms for multi-lateral cooperation.

B - Priority research towards borderless issues

The following priorities are issues towards security, protection, crisis management, taking into account complexity and scalability and multidisciplinary aspects.

B - 1 - Technological researches to increase trustworthiness

Technological support to achieve digital credibility will be the cornerstone to make the digital ecosystem viable. Technological support is indispensable for translating governance policies and business rules in the practices and operations, due to new complexity and scalability.

Threat analysis, propagation

Analysis of the threat landscape and vulnerabilities, in an interconnected and convergent digital society

- ✓ **Threats analysis**: study of the threats landscape in an interconnected and convergent digital society. There is more and more interconnectivity of different kind of infrastructures. This convergence together with the complex nature of highly connected systems may give birth to grey areas in the security threats landscape.

Virtual paradigm

Development of audit mechanisms and digital investigations tools for a virtual world, within the context of globalisation of criminals and their targets.

- ✓ **Digital forensics**: development of new methodologies and tools to meet the requirements of performing digital investigations of cyber world, considering the characteristics of virtualisation of computing and storage resources besides globalisation of criminals and their targets. Post-incident investigations are very important to analyse the perpetrators of digital crimes and to prosecute them for their activities.
- ✓ **Audit mechanisms**: development of audit mechanisms for a virtual world. Its use by mission-critical industries require a corresponding set of monitoring and auditing techniques that can provide reliable testing of the effectiveness of security capabilities of these infrastructures.

Massively computing paradigm

Development of new traffic management models to deal with 'rush hour' flow management especially in the advent of emergencies.

- ✓ **Cloud security**: investigation of the *Cloud danger* to provide a pragmatic view of the opportunities vis-à-vis the vulnerabilities of this borderless computing paradigm. Some stakeholders are overlooking the prevailing extent of cloud security concerns; whereas others are sceptical to take part in cloud-centric opportunities.
- ✓ **Cloud risk metrics**: development of 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.

✓ **Traffic management during crisis**: development of new traffic management models to deal with 'rush hour' flow management especially in the advent of emergencies. 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.

Mobility and borderless computing paradigm

Investigation of the Cloud danger to provide a pragmatic view of the borderless computing paradigm

Evaluation of the impact of regulations on the cloud business model needs.

B - 2 - Organisational priorities to manage crisis

Contingency plans, continuity of service

Development of contingency plans to avoid alarm in the case of any high profile cyber incidence, and preparation for any adverse situation to cope with the aftermaths of a possible outage or serious depletion of digital resources.

Investigation of the readiness of operational critical infrastructures to ensure resilience and to deliver minimum services.

✓ **Contingency plan**: development of 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'). Panic management among the population in the advent of any major disaster arising from ICT. 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.

✓ **Crisis management**: investigation of the readiness of operational critical infrastructures to respond to the emerging threats, to ensure resilience and 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.

✓ **Dependency metrics**: 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.

✓ **Chaos management**: preparation for any adverse situation to cope with the aftermaths of a possible outage or serious depletion of digital resources, through a global cooperation to have access to some minimum resources outside the disaster zones that could be accessed via satellites to manage recovery and restoration operations. 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.

B – 3 - Legal priorities to enhance legal framework and to design institutional observatory

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.

Cyber-deterrence framework

Implementation of a cyber-deterrence framework, and modalities including legal and constitutional implications.

- ✓ **Deterrence framework**: implementation of a cyber-deterrence framework that requires adequate support for the technological developments and support of policies and tools to enforce these policies in order to achieve the operational control.
- ✓ **Cyber-deterrence legislative implementation**: development of the framework and modalities including legal and constitutional implications for cyber-deterrence. A number of countries may require legal or constitutional changes to erect 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.
- ✓ **Regulatory harmonisation**: harmonisation of national/continental regulatory initiatives at the global scale as their disparities gives birth to cyber paradises. The cooperation between governments towards a unified set of regulations for cyberspace, where geo-political borders are already diminished, in the day-to-day conduct of business, must address the possibilities, in the event of trouble and dispute, for legal loopholes and jugglery that could overwhelm the stakeholders.
- ✓ **Cyber-deterrence concept and impact**: governments should facilitate targeted and specialised consultation on the concept of cyber deterrence and its impact on the global security landscape. The first step towards the readiness of nations to deal with cyber threats is to maintain a credible level of cyber-deterrence. Political manoeuvrings often use deterrence as a negotiation chip to settle issues. This includes the impact analysis of cyber deterrence in the emerging geopolitical landscape of the world politics.
- ✓ **Digital evidence usage**: early serious initiatives to launch the preparation and consequent adoption of legislation in order to facilitate the use of digital evidence in courts of law. The preparation phase will require a multi-domain approach to resolve the soundness and the acceptability of digital evidence without compromising the social rights of citizens and policing issues (how to collect and preserve evidence in a 'virtual world').

Emergency response

Digital security task forces at national and international levels with clearer distinction of the roles of actors such as CERTs, Intelligence Agencies.

- ✓ **Digital security task forces**: 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.

Cyber-policy (surveillance and control) and digital dispute

Design of data ownership rules, of transparent cyber-policing rules including virtual border-controls, of a global digital dispute analysis and resolution.

Design of a framework for corporate dispute analysis of digital assets.

- ✓ **Disputes analysis**: design of a framework for corporate dispute analysis of digital assets. This framework will not motivate stakeholders to take cyber revenge, as there will be a better outlet to resolve corporate disputes, resulting from claims on digital asset, in a more logical way without harming the security of their rival's digital assets.
- ✓ **Data ownership**: renegotiation of data ownership rules as more and more data is accessible to a range of public and private actors. The controlling of the processing of such data requires redefinition of data ownership rules in these cyberspaces: responsibility of a data owner and control of the data usage by its controller.
- ✓ **Cyber-policy**: development of transparent cyber-policing rules including virtual border-controls in the digital world. The demarcation of responsibilities for cyber-protection requires some distinctive boundaries for the various agencies and departments that are different from geo-political borders.
- ✓ **Dispute analysis**: development of a global digital dispute analysis and resolution framework to resolve conflicts among the participating entities. Any cooperation initiative results in difference of opinions and approaches that often lead to disputes of variable severity.
- ✓ **Cloud operating regulations**: development of suitable security audit of best practices for cloud infrastructures and of some 'operating permit' to cloud service operators. The issuance of such authorisations will require some controls to be carried out.

Cyber-criminality

An effective anti-cyber laundering initiative will deter criminals and help authorities to identify new kind of frauds.

- ✓ **Data and information flow agreement**: the flow of data and information across the geopolitical borders require some global 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, but it can be achieved by taking all the stakeholders on board.
- ✓ **Anti-cyber laundering initiative**: an effective anti-cyber laundering initiative will deter criminals and help authorities to identify new kind of frauds. 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.

Consequently, the following long term recommendations (or future actions) were suggested in Deliverable D3.1 - Interim recommendations report on future global research challenges in ICT trust and security. By long term, we were referring to taking place in the Horizon 2020 work programme.

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.