BUILDING International Cooperation
for Trustworthy ICT

D2.4 – Report on prioritized Trust and Security themes

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 James Clarke

Tel: +353 71 9166628

Fax: + 353 51 341100

E-mail: jclarke@tssg.org

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

Table of Contents

1 - Executive Summary 4
2 - Introduction 8
3 - Challenges for international cooperation in trustworthy ICT 9
3.1 The changing landscape of security research 9
Threats are more and more related to massive usage of the network 9
Outsourced data storage and virtualization remain a major security challenge 9
Massive networked phenomena bring another order of magnitude in protection complexity 10
Some fundamental concepts are not yet fully expressed in computer science terms 10
3.2 The moving landscape of attacks, surveillance and failures 10
The enlarged spectrum of attackers 10
The underlying cyber-war between countries 12
The surveillance of networks, and people activity 12
4 - Ranked priority research in ICT trust and security 13
4.1 Internet penetration and Networked Readiness Index 13
4.1.1 Brazil 16
4.1.2 India 18
4.1.3 South Africa 20
4.2 Brazil – EU priority research areas in Trustworthy ICT 22
4.3 India – EU priority research areas in Trustworthy ICT 31
4.4 South Africa – EU priority research areas in Trustworthy ICT 40
4.5 Mapping of ranked priority research (Brazil, India, South Africa versus EU) 46
5 - Conclusions 54
6 - References 57

List of Tables

Table 1. Ranked priority research topics 5
Table 2. Key challenges of the Future Internet addressed in H2020 6
Table 3. Mapping between long term recommendations and priorities. 7
Table 4. Internet penetration 13
Table 5. Mapping of EU and BIC countries research agendas in ICT Trust and Security 53
Table 6. Ranked priority research topics 54
Table 7. Key challenges of the Future Internet addressed in H2020 55
Table 8. Mapping between long term recommendations and priorities. 56

List of Figures

Figure 1. Infection rates by country/region in 4Q12 , by CCM (computers cleaned per mile) - Microsoft 11
Figure 2. Phishing sites per 1,000 Internet hosts for locations around the world in 4Q12 - Microsoft 11
Figure 3. Network Readiness Index (NRI) 14
Figure 4. Network Readiness of BRICS countries 15
Figure 5. Brazil: Networked Readiness Index 2012 and Rank (out of 142 countries).....17
Figure 6. India: Networked Readiness Index 2012 and Rank (out of 142 countries).....19
Figure 7. South Africa: Networked Readiness Index 2012 and Rank (out of 142 countries) .21
Figure 8. Malware and potentially unwanted software categories in Brazil in 2012, by percentage of computers reporting detections (Microsoft Security Intelligence Report)).....24
Figure 9. National Identity card in Brazil 28
Figure 10. Malware and potentially unwanted software categories in India in 2012, by percentage of computers reporting detections (Microsoft Security Intelligence Report)).....33
Figure 11. Malware and potentially unwanted software categories in South Africa in 2012, by percentage of computers reporting detections (Microsoft Security Intelligence Report)).....42
Figure 12. African Undersea Cables in Africa (2014).....45

1 - Executive Summary

The purpose of the BIC coordination action project is fostering cooperation across the international funding agencies and researchers within the focus areas of ICT Trust and Security, 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 BIC project, though their International Advisory Group (IAG) and the Working Group 3 (Programme /funding focus/ identify community), has been actively promoting a strategic approach advocating the need for a more strategic multi-lateral cooperation model in addition to the current tactical bi-lateral models, for international cooperation in trustworthy ICT [1], [2]. As a result, a new extended working group (EWG) model has been proposed by the IAG members based on the extension of the original BIC model of IAG and core working groups including an Extended Working Group (EWG) in each country. In this proposed structure, Extended Working Groups (EWGs) are defined as the country specific arms of the Core Working Group (CWG) of BIC. Although outside the original scope of BIC, the India members of the IAG and WG3 have spearheaded this model already and held a kick off meeting of their EWG in New Delhi during this period with the support of the BIC project, India government and the European Commission delegate in New Delhi [9]. With this impetus, the EWG initiative is now being initiated in the other BIC countries, Brazil and South Africa. This deliverable was taking place in parallel, and, therefore, was used for a dual purpose: to compile, prioritise and rank the bi-lateral research topics for each country and analyse alongside the EU priorities, and as a launching pad terms of reference document for each BIC country's EWG start up and initiation phase white paper.

This deliverable is a report on ranked priority research on future global research challenges in ICT trust and security. It takes into account the workshops and meetings organised by the project and the working groups. Special emphasis is given on the new entrants to the INCO community (via the BIC project) Brazil, India and South Africa, whereby the project developed, along with IAG and WG members from each country, a working document describing the ranked prioritised ICT Trust and security research topics from their perspectives. In addition, these documents were used during the start-up and establishment phases of External Working Groups (EWG) in each of the BIC countries.

Cyber security has become a major issue in all countries, including BRICS countries. It applies to all governments, all businesses and all network users, even if the technical measures are not fully implemented to the risk, especially for small businesses. Cyber security and resilience became the first priority in all industrialized countries and emerging economies. The priorities of research in ICT trust and security are then placed privacy, transparency, for the internet actors, especially for Europe, and then mobile security, trust, identity management as challenges for 2020, for the emerging countries. Cloud security, intellectual property, ownership, accountability, cryptography on digital signature or authentication, are research topics that derive from the previous priorities. Issues such as green security, cascading failures of infrastructures, are barely mentioned, but it should be noted that this could indeed be due to a lack of participation of experts from these fields.

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 localization 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 BRICS countries (especially the BIC countries of India, South Africa, Brazil), priorities are rather security in real-time from a mobile device. In addition, recent research has shown the need to take into account culture and history of the country to implement models of trust and reputation in connection with security mechanisms in the exchange of e-commerce.

Table 1 contains the ranked priority research topics in ICT trust and security after compiling the national topical interests of each country in particular and then mapping with the EU prioritised themes. The ranking was based on the coverage amongst the participating countries and the relevance of the topic within each country.

Topic 1 : Research in Cyber security

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, linkage with privacy mechanisms, 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.

Table 1. Ranked priority research topics

The Horizon 2020 programme will need to take into account the balance between technological dimensions, diversity, interoperability, on the one hand, and usability and flexibility, on the other hand. Table 2 categorises these topics around key challenges of the Future Internet, which will also need to be addressed within Horizon 2020.

Challenge 1. Diversity and interoperability

An ecosystem in the global geography with diversity of cultures and contexts;

Challenge 2. Flexibility and innovation

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

Challenge 3. Trustworthiness

Strengthening the resilience of infrastructure control and crisis management;

Challenge 4. Transparency

Governance and digital control, in Europe and worldwide and digital multi-lateral governance at global scale, neutrality of the entire ecosystem, not just net neutrality;

Challenge 5. Freedom, Openness, Ethics

Principles of human values, flexibility and usability, architecture and usage interrelation and feedback, building together a cyber-ethics;

Challenge 6. 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;

Challenge 7. Trust and Privacy

Digital industrial policy, restoring confidence and privacy, intimacy of cloud computing, repositioning trust infrastructure at the same level as security infrastructure.

Table 2. Key challenges of the Future Internet addressed in H2020

In the BIC Deliverable D3.1 [3], we already listed an initial set of long-term recommendations (2015-2020). As shown in Table 3, the mapping between the ranked priorities and the long-term recommendations may be grouped according the following partitions.

Societal:

- Cyber security : 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:

- Cyber security : 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:

- Cyber security : 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;
- Appropriate mechanisms for effective INCO, including bi-lateral and multi-lateral cooperation models needed for Cyber security;
- A longer term strategy including coordination, flexibility, and providing for longer durations of continuity is required for maximum impact.

Table 3. Mapping between long term recommendations and priorities.

This research topic prioritisation work will be continued in a number of upcoming internal country External Working Group (EWG) meetings and will be incorporated into the next version of D3.2. Final recommendations report, before being presented at the final International Advisory Group (IAG) meeting.

2 - Introduction

An international vision of the digital security is essential because the ICT ecosystem is a continuum, a territory without borders, where the laws of any country are increasingly difficult or impossible to enforce. A multidisciplinary vision of digital security is also important because the ecosystem is a cyber-social meta-system, where culture and behaviour are different depending on socio-economic situation, context and country. It is therefore necessary to bring together all relevant disciplines – technology, law, economy, criminology, philosophy, linguistics, psychology and sociology – if there is to be a holistic framework that can span all the cross-cutting issues.

This BIC report provides a survey and an analysis of the ranked priority research of the new entrants in international cooperation, Brazil, India and South Africa, in order to develop a deeper understanding of important themes and topics that need to be tackled on a global basis in order to strengthen the EU's international collaborations within Trustworthy ICT, including the Trust, Security & Privacy areas. The end goal is to contribute to a trusted and secure global digital communication and information handling – i.e. a secure and dependable international ICT infrastructure. This setup will be based on an evolving Internet, together with the many services that rely on it to deliver their benefits.

Report Structure

This deliverable is organised in the following sections:

Section 3, entitled Challenges for international cooperation in trustworthy ICT and gives a view of the landscape, summarising the new threats and vulnerabilities of the digital ecosystem due to the evolution of technology and usages.

Section 4, entitled Ranked priorities research in ICT security, describes and examines the priorities in ICT security research from the BIC Countries Brazil, South Africa and India.

Section 5, entitled Conclusions summaries the priority topics for international cooperation in ICT trust and security, and key challenges of research for international cooperation to be carried out in Horizon 2020.

3 - Challenges for international cooperation in trustworthy ICT

This section examines the new challenges for international cooperation in trustworthy ICT, following the recent landscape of security research and the new spectrum of attacks and failures, due to new threats and vulnerabilities of the digital ecosystem and to the evolution of technology and usages.

3.1 The changing landscape of security research

Threats are more and more related to massive usage of the network

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, within 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.

Outsourced data storage and 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 given 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 these issues can only be addressed on an international level. Moreover, for the whole area of cyber forensics, evidence and accountability, International cooperation is necessary as data centres are located worldwide and, therefore, the need for law enforcement to work transparently across borders. Additionally, interoperability is needed between standards used by different agencies for cyber forensic data [4].

Massive 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 terminals), 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.

Some fundamental concepts are not yet fully expressed in computer science terms

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, especially within the EU. 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 [1].

3.2 The moving landscape of attacks, surveillance and failures

The enlarged spectrum of attackers

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 are on the rise. The target is not necessarily the computer object but often the image of this object. Gaining of 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. Figure 1 and Figure 2 show some illustrative data points to highlight the situation [5].

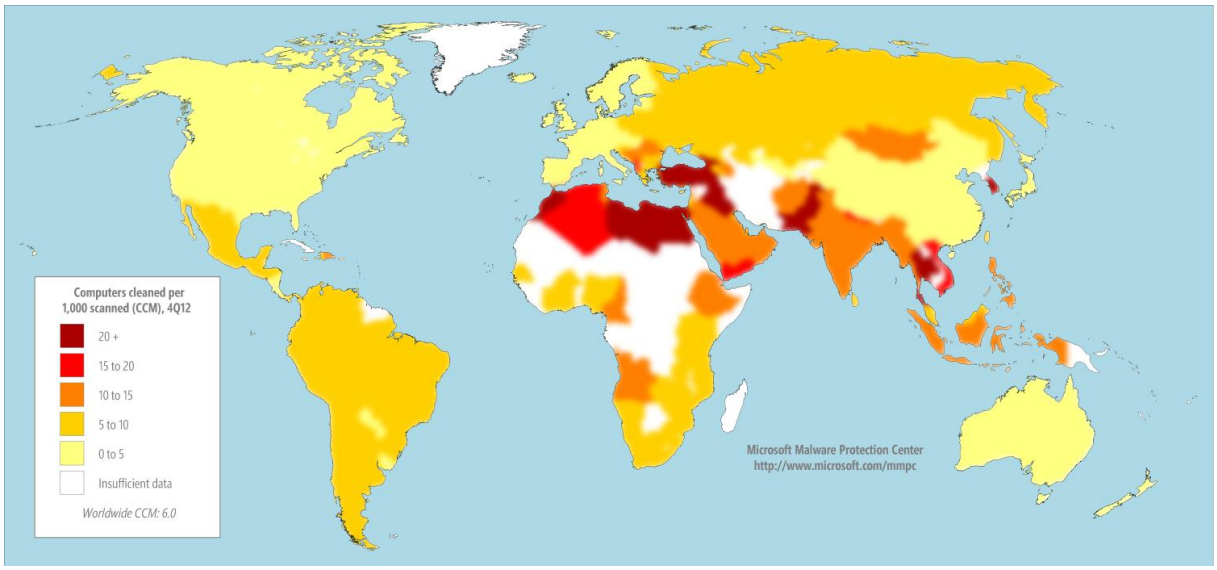


Figure 1. Infection rates by country/region in 4Q12 , by CCM (computers cleaned per mile) - Microsoft[1]

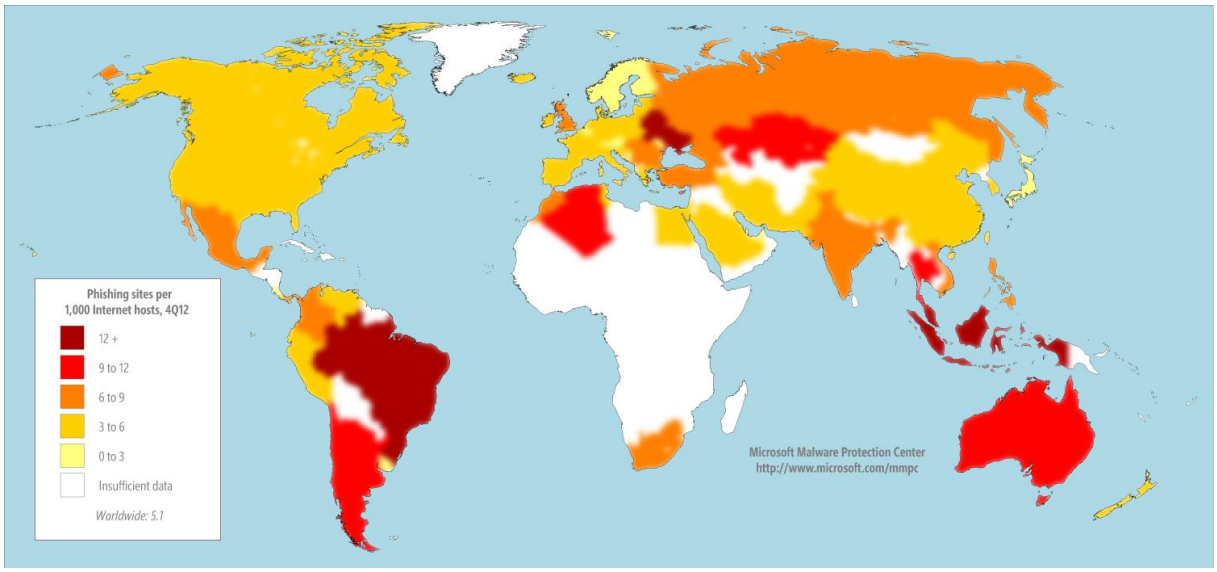


Figure 2. Phishing sites per 1,000 Internet hosts for locations around the world in 4Q12 - Microsoft[2]

[1] Global infection rates: telemetry data generated by Microsoft security products (Microsoft Security Intelligence Report, Volume 14).

[2] Global distribution of phishing sites : phishing sites are hosted all over the world on free hosting sites, on compromised web servers. (Microsoft Intelligence Report, Volume 14).

The underlying cyber-war between countries

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[3]. Furthermore, 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 cyber security, some of the countries have already started working together.

The surveillance of networks, and people activity

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 United 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.

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

4 - Ranked priority research in ICT trust and security

This section examines the research priorities from the BIC Countries Brazil, South Africa and India on a bi-lateral basis and makes a start at mapping these towards multi-lateral cooperation.

4.1 Internet penetration and Networked Readiness Index

Before describing the various priorities in ICT trust and security research of Brazil, India and South Africa, it is important to recall the actual digital situations of these different countries, to understand the selection of these priorities. Table 4 below gives the Internet penetration of the BRICS countries (Brazil, Russia, India, China, South Africa), with the figures of some other countries (United States, Japan, Germany, United Kingdom, France, Italy, Spain and Nigeria) as milestones [6].

#	Country or Region	Population, 2012 Estimation	Internet Users Year 2000	Internet Users Latest Data	Penetration (% Population)	Users % World
1	China	1,343,239,923	22,500,000	538,000,000	40.1	22.4
2	United States	313,847,465	95,354,000	245,203,319	78.1	10.2
3	India	1,205,073,612	5,000,000	137,000,000	11.4	5.7
4	Japan	127,368,088	47,080,000	101,228,736	79.5	4.2
5	Brazil	193,946,886	5,000,000	88,494,756	45.6	3.7
6	Russia	142,517,670	3,100,000	67,982,547	47.7	2.8
7	Germany	81,305,856	24,000,000	67,483,860	83.0	2.8
9	United Kingdom	63,047,162	15,400,000	52,731,209	83.6	2.2
10	France	65,630,692	8,500,000	52,228,905	79.6	2.2
16	Italy	61,261,254	13,200,000	35,800,000	58.4	1.5
18	Spain	47,042,984	5,387,800	31,606,233	67.2	1.3
						Users % Africa
	Nigeria	170,123,740	200	48,366,179	28.4	28.9
	South Africa	48,810,427	2,400,000	8,500,000	17.4	5.1

Table 4. Internet penetration[4]

[4] http://www.internetworldstats.com/stats.htm

The Global Information Technology Report (GITR)[5] analyses in detail the main drivers and impacts of this ICT-enabled hyper-connected world and contributes to the work of the World Economic Forum's recently launched Hyper-connected World Initiative, which establishes a means of understanding the systemic nature of change in a connected world [7].

Through the lens of the Networked Readiness Index (NRI) as shown in Figure 3, the driving factors and impacts of networked readiness and ICT leveraging have been identified, highlighting the joint responsibility of all social actors, individuals, businesses, and governments. Figure 4 shows the NRI specifically for BICS countries.

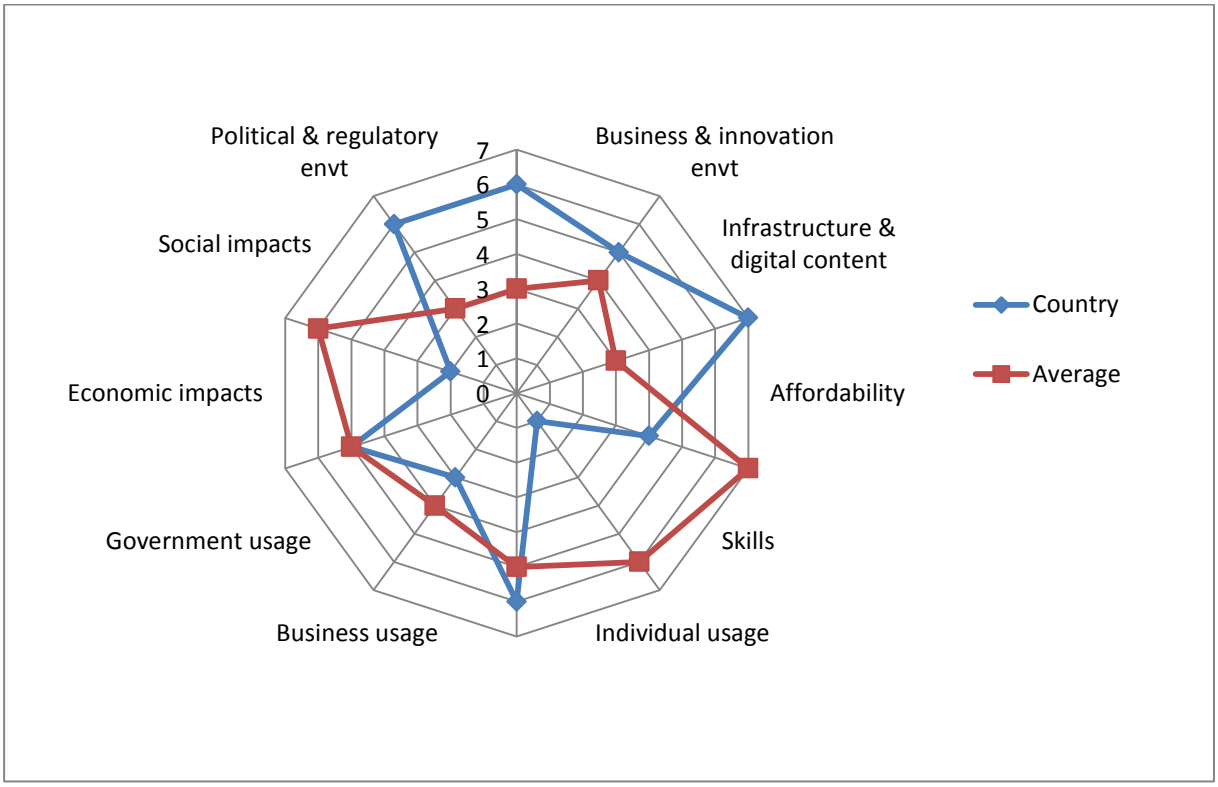


Figure 3. Network Readiness Index (NRI)

[5] The GITR series has been published by the World Economic Forum in partnership with INSEAD since 2002, accompanying and monitoring ICT advances over the last decade as well as raising awareness of the importance of ICT diffusion and usage for long-term competitiveness and societal well-being.

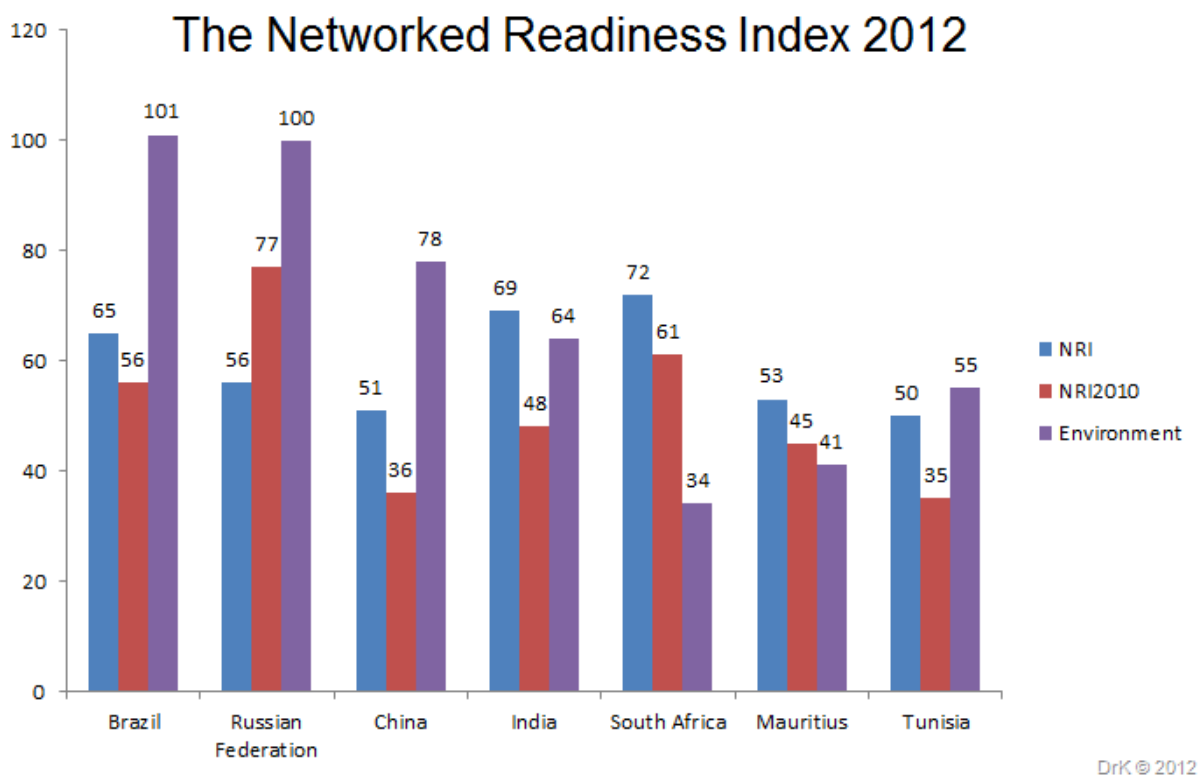


Figure 4. Network Readiness of BRICS countries[6]

The Network Readiness Index for the BIC countries Brazil, India, and South Africa is now analysed in the following pages.

[6] http://khomotsok.files.wordpress.com/2012/05/image12.png

4.1.1 Brazil

Networked Readiness Index 2012: 65 out of 142.

Average Score: 3.9 out of 7

Brazil, positioned narrowly above the middle range of our rankings at 65th place out of 142, benefits from strong levels of business ICT usage. These, combined with fairly advanced levels of technological capacity in particular segments of its industry, allows the country to achieve one of the strongest performances of ICT-enabled innovations in the region, both in terms of new products and services and more efficient processes. Notwithstanding these strengths, its overall business environment with its burdensome procedures to create new businesses and its high tax rates, in addition to its high mobile cellular tariffs and poor skill availability, hinder the potential of the Brazilian economy to fully benefit from ICT and shift toward more knowledge-based activities at a faster pace. The success of smartphones extends beyond developed regions. In Brazil, for example, the smartphone's share in monthly 3G handset sales rose from 45 per cent in May 2010 to 76 per cent in May 2011, tripling in terms of unit volumes during the same period.

In Brazil, the telecommunications sector government agencies have a long-standing and active engagement with industry, utilizing mechanisms such as public consultations and keeping an on-going dialogue on key issues. The Ministry of Communications and ANATEL, the National Telecommunications Agency, are very active in key international policy and regulatory organizations that are working to address mobile communications. By including industry in the decision-making process, the results better reflect the needs of both the government's objectives and the private sector's interests. ANATEL is an example of a regulator that has proactively taken steps to manage spectrum in order to maximize frequency harmonization at the international level and leverage economies of scale. In addition, some of the objectives of Brazil's National Broadband Program (PNBL), Connected Brazil, are to create opportunities, speed up economic and social development, promote social inclusion, reduce social and regional differences, and promote job creation and capacity building for the population to use information technologies. The Connected Brazil Forum is composed of almost 60 institutions from diverse sectors, public and private, and directly linked with broadband program goals. Mobile communications will play a pivotal role in fulfilling PNBL's theme of a "fast Internet for all of Brazil" and aid in accelerating mobile broadband access and adoption, increasing local applications development, and decreasing device and service costs. Learning from modelling and other economic data, many countries, including Brazil, have made strategic investments in the ICT industry. These investments are designed to create new jobs, increase revenue for the government, and provide more stable overall economies.

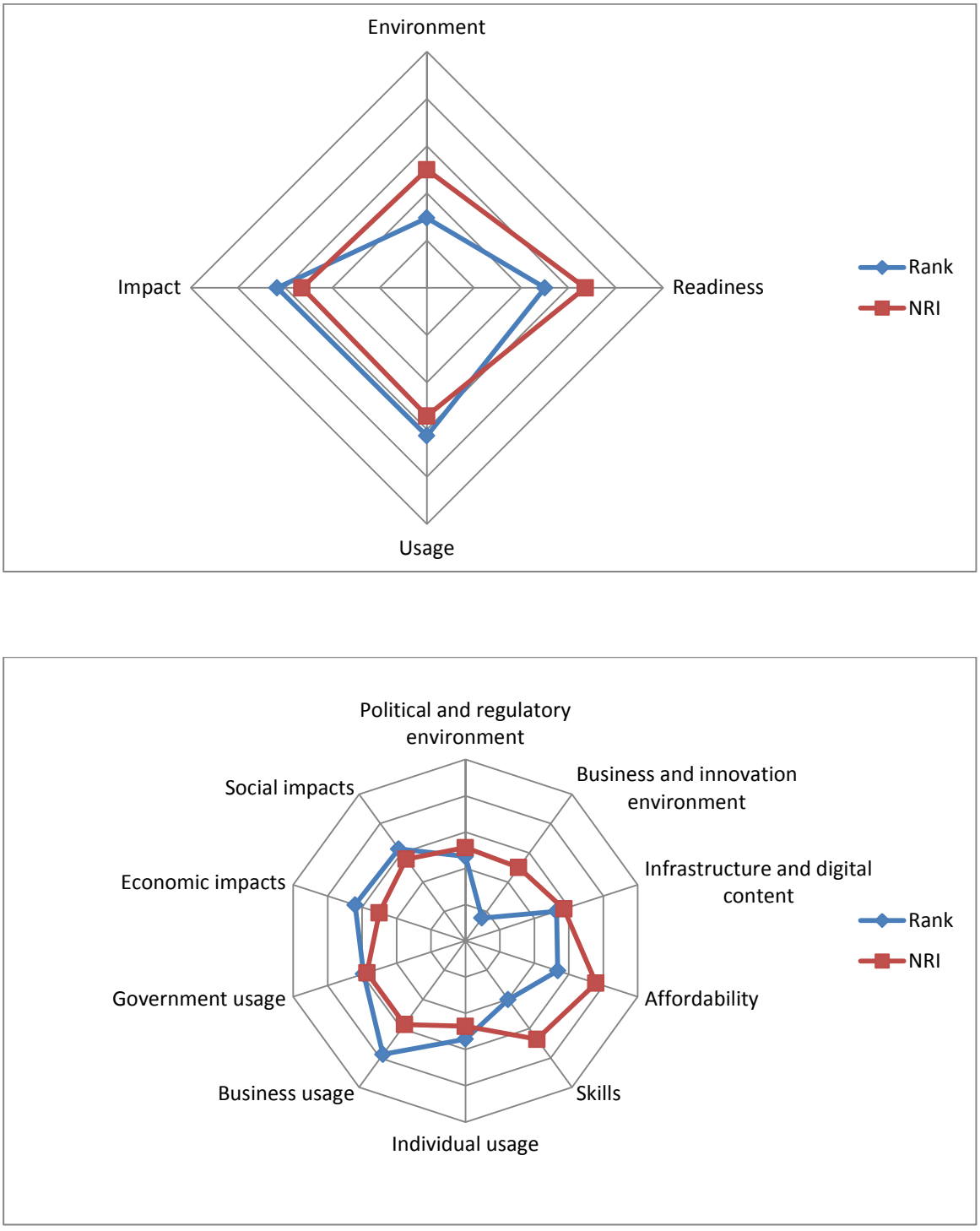


Figure 5. Brazil: Networked Readiness Index 2012 and Rank (out of 142 countries)

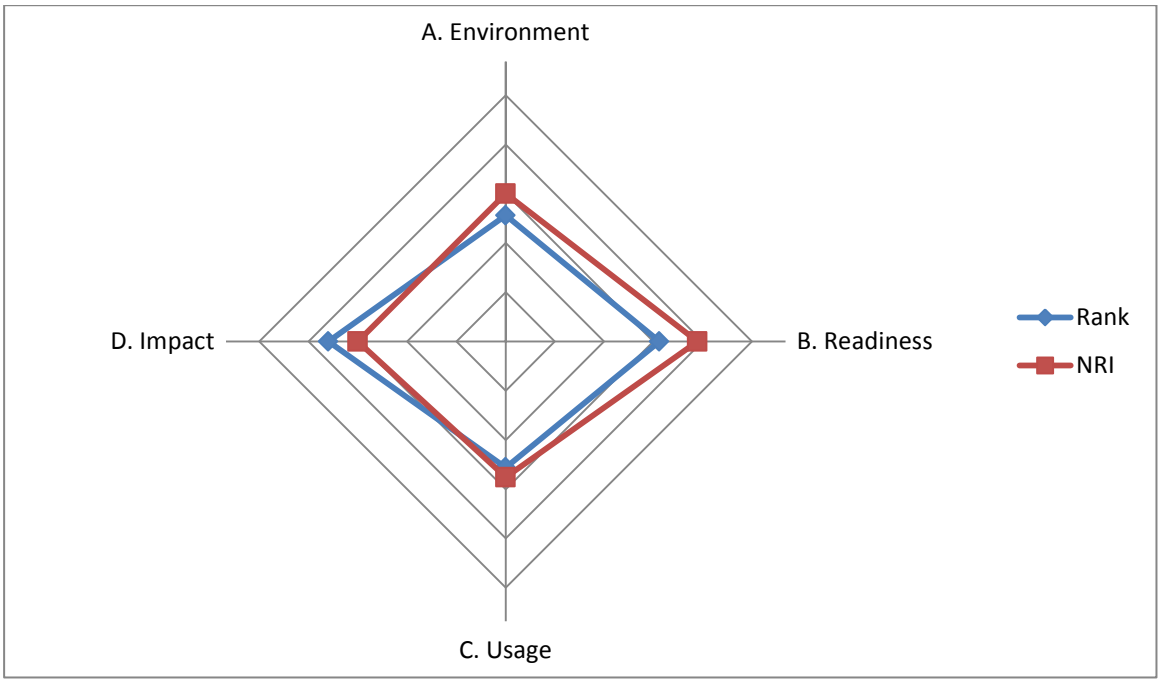
4.1.2 India

Networked Readiness Index 2012: 69 out of 142.

Score: 3.9 out of 7

Almost 20 ranks behind China, India at 69th place overall delivers a very mixed performance, with encouraging results in a few areas and a lot of room for improvement elsewhere, notably in the political and regulatory environment and the business and innovation environment. Extensive red tape stands in the way of businesses and corporate tax is among the highest of all analysed countries. For instance, it typically takes four years and 46 procedures to enforce a contract. Starting a business is longer and requires more paperwork than in most countries. Other variables in the environment sub-index are better assessed, including the availability of new technologies, the availability of venture capital, the intensity of local competition, and the quality of management schools. One of the weakest aspects of India's performance lies in its low penetration of ICT. The country ranks 117th in the individual usage pillar. There are 61 mobile subscriptions for every 100 population, a relatively low figure. A mere 7.5 per cent of the population uses the Internet. Six per cent of households own a PC and broadband Internet remains the privilege of a few, with less than one subscription per 100 population. Upgrading skills and infrastructure would contribute to increasing these figures. Already, fierce competition and innovations for the "bottom of the pyramid" have made India the leader in the affordability pillar, thus providing a significant boost to the country's readiness. Although penetration is still limited among the population at large, businesses are early and assiduous adopters of new technologies. And the government is placing a great deal of emphasis on ICT as a way to address some of the country's most pressing issues, including job creation, corruption and red tape, and education. Whether this vision will translate into a transformation of the economy and society remains to be seen. But already ICT is having a —small— transformational impact on the economy, which is partly reflected in India's performance in the economic impacts pillar.

Mobile broadband growth is particularly accelerating in emerging countries, rising from 61 per cent of all broadband connections in these regions in 2011 to 84 per cent in 2016. At this pace, emerging regions will surpass the developed world in terms of the number of mobile broadband connections in first half of 2013. In India, for example, mobile broadband became available in late 2009. Less than 18 months later, the number of subscriptions over mobile broadband networks surpassed the number of fixed broadband subscriptions. Usage has been with mobile devices rather than PCs.



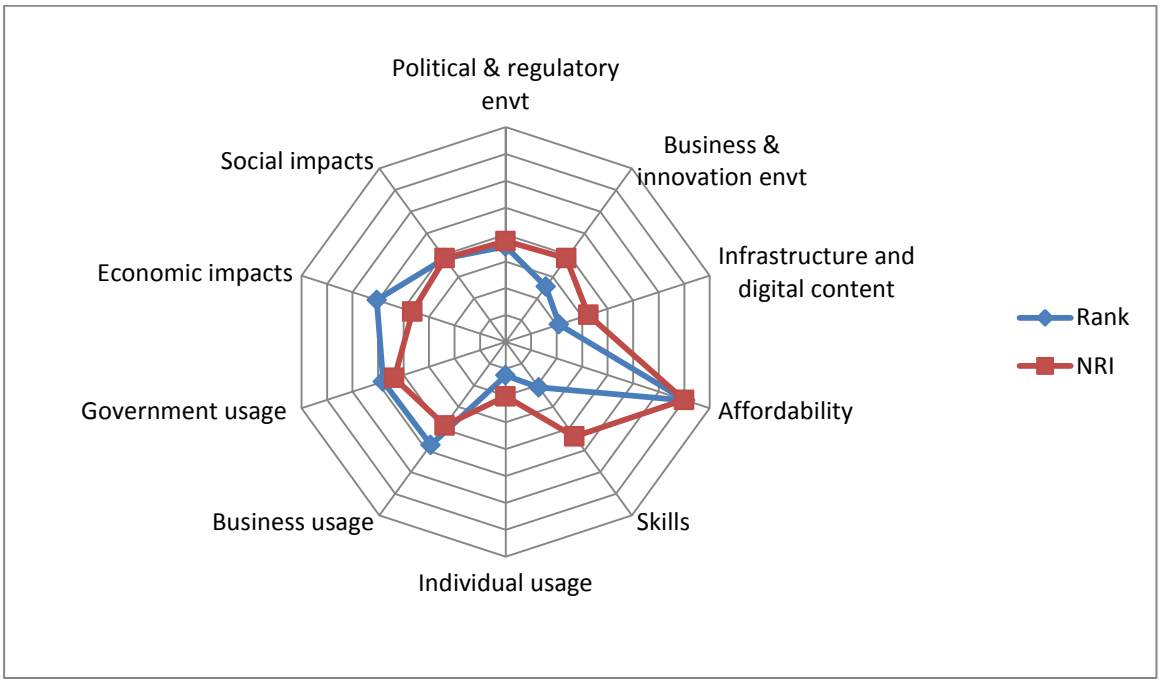


Figure 6. India: Networked Readiness Index 2012 and Rank (out of 142 countries)

4.1.3 South Africa

Networked Readiness Index 2012: 72 out of 142.

Score: 3.9 out of 7

Despite counting on one of the most solid political and regulatory environments and better framework conditions for entrepreneurship and innovation in the region, South Africa, at 72nd place, is not yet leveraging the potential benefits associated with ICT. Important shortcomings in terms of basic skills availability in large segments of the population and the high costs of accessing the insufficiently developed ICT infrastructure result in poor rates of ICT usage, despite efforts on the part of the business community to use ICT and integrate it in a broader, firm-based innovation system. As a result, the economic impacts accruing from ICT are patchy and the social impacts disappointing. Upgrading the overall skills at all layers of society and increasing efforts to build affordable infrastructure for all would allow the country to increase its ICT readiness and uptake and, in turn, spread its impacts across society. A pilot project in South Africa demonstrates how smartphones and mobile broadband technologies can be leveraged by nurses to improve access to healthcare within underserved communities. Merging the best of both the computing and mobile worlds, advanced smartphones and tablets represent a new, highly personalized, rich computing experience.

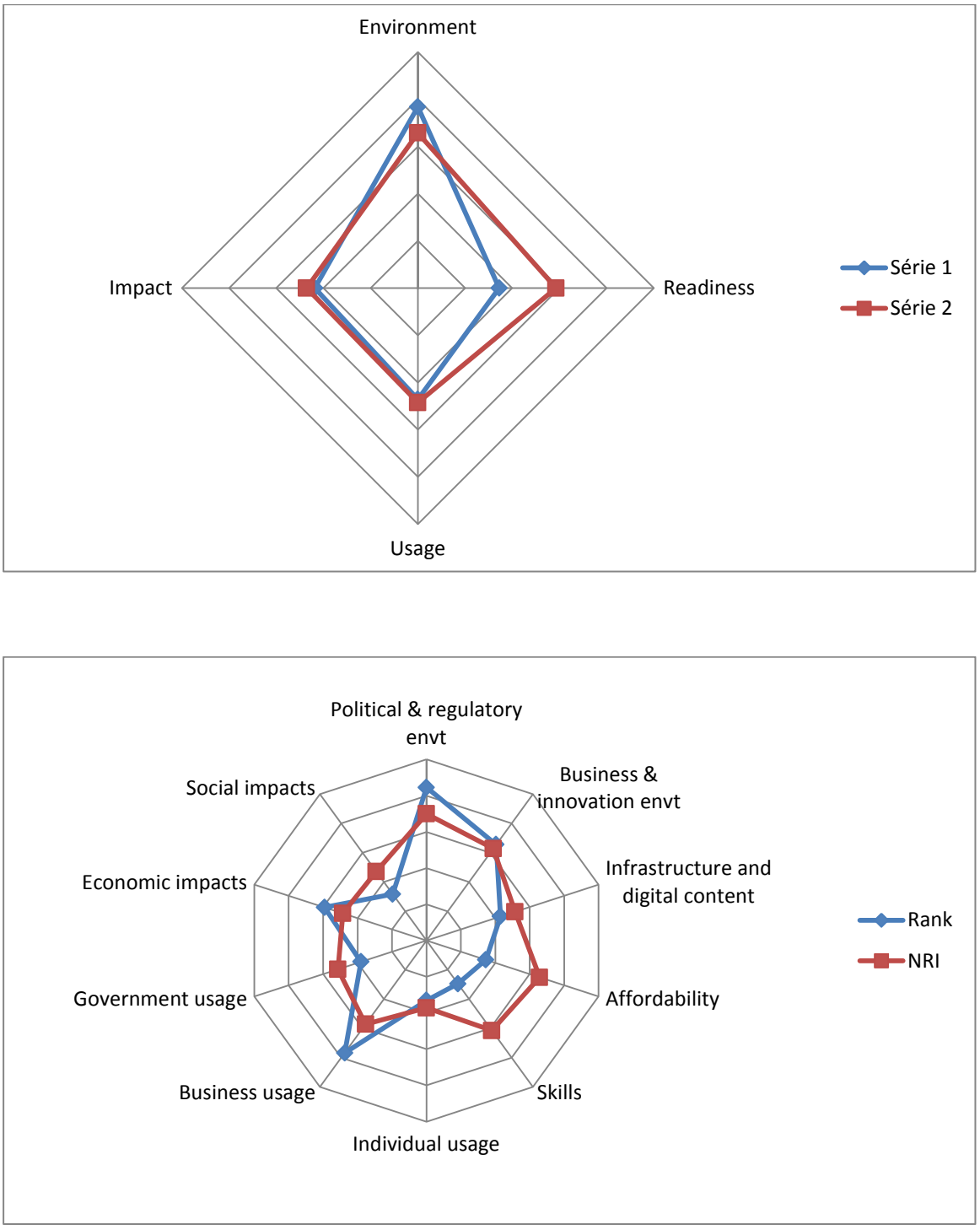


Figure 7. South Africa: Networked Readiness Index 2012 and Rank (out of 142 countries)

4.2 Brazil – EU priority research areas in Trustworthy ICT[7]

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 Cyber Security

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 cyber security:

- **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 cyber-security 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 cyber security**: 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 also allow the data exchange between EU and Brazil to analyse cybercrime and share experiences.

[7] 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.

- **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 cyber security and training, and joint research activities to foster collaboration between international and national, agencies as well as the private sector, are required. Multi-polar cyber security 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 cyber security strategy will be significant efforts to harmonise the cyber security 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 Cyber security.
- **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 8 shows the

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

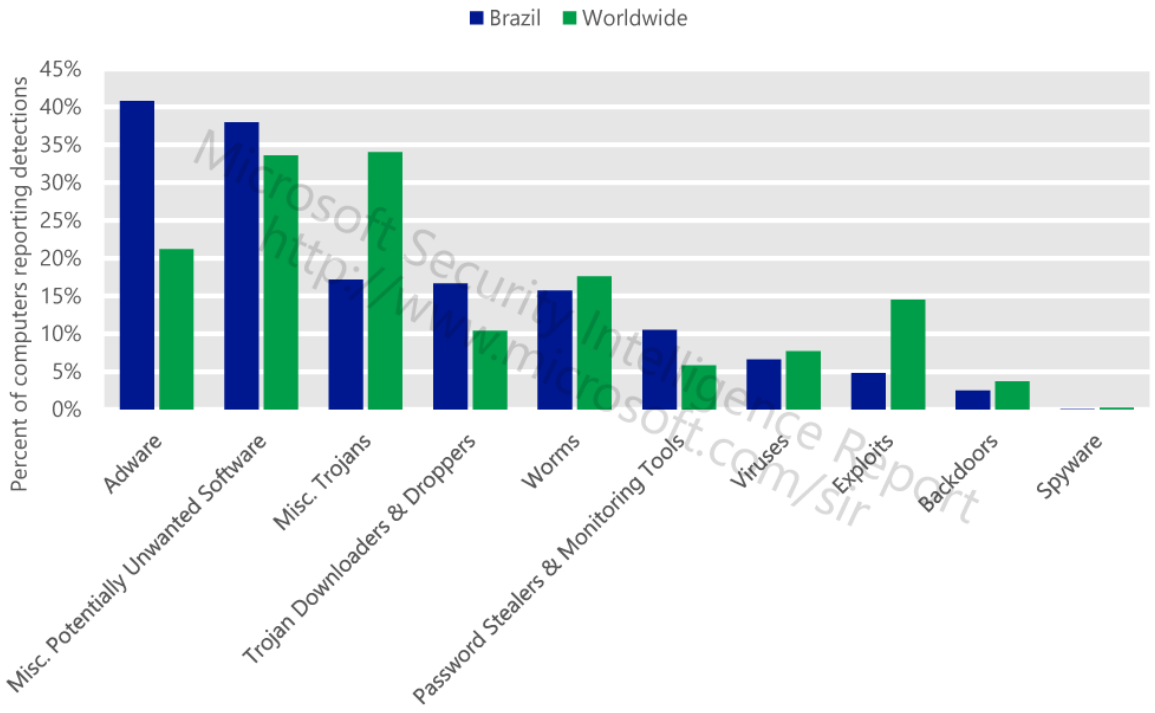


Figure 8. Malware and potentially unwanted software categories in Brazil in 2012, by percentage of computers reporting detections (Microsoft Security Intelligence Report))

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 Brasil – 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 9. 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 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.

- **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.

4.3 India – EU priority research areas in Trustworthy ICT[8]

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 Cyber Security

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

- 7th February, 2013. The EU Cyber security Strategy of the European Union: *An Open, Safe and Secure Cyberspace*[9], was published.
- 9th May, 2013: India's National Cyber Security Policy was approved by the Government of India[10];
- 2nd July, 2013. India's National Cyber Security Policy[11] was formally notified.

The approaches of both EU and India towards cyber security 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 Cyber security 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 cyber security, 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 cyber security:

- 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.

[8] 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.

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

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

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

- Appropriate regulations: Policy makers must find appropriate regulations in order to coordinate efforts from different stakeholders to try to develop a roadmap of cyber-security practices that will be sharpened in the future in order to ensure a leading role of Europe and India together in the global digital economy. ***[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 Cyber-security Laws - Dr. Jaijit Bhattacharya, Director, Government Advisory, Hewlett Packard.]***
- International Data Exchange for cyber security: 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 cyber security 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 cyber security strategy will be - significant efforts to harmonise the cyber security

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 10 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 cyber-security 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]***

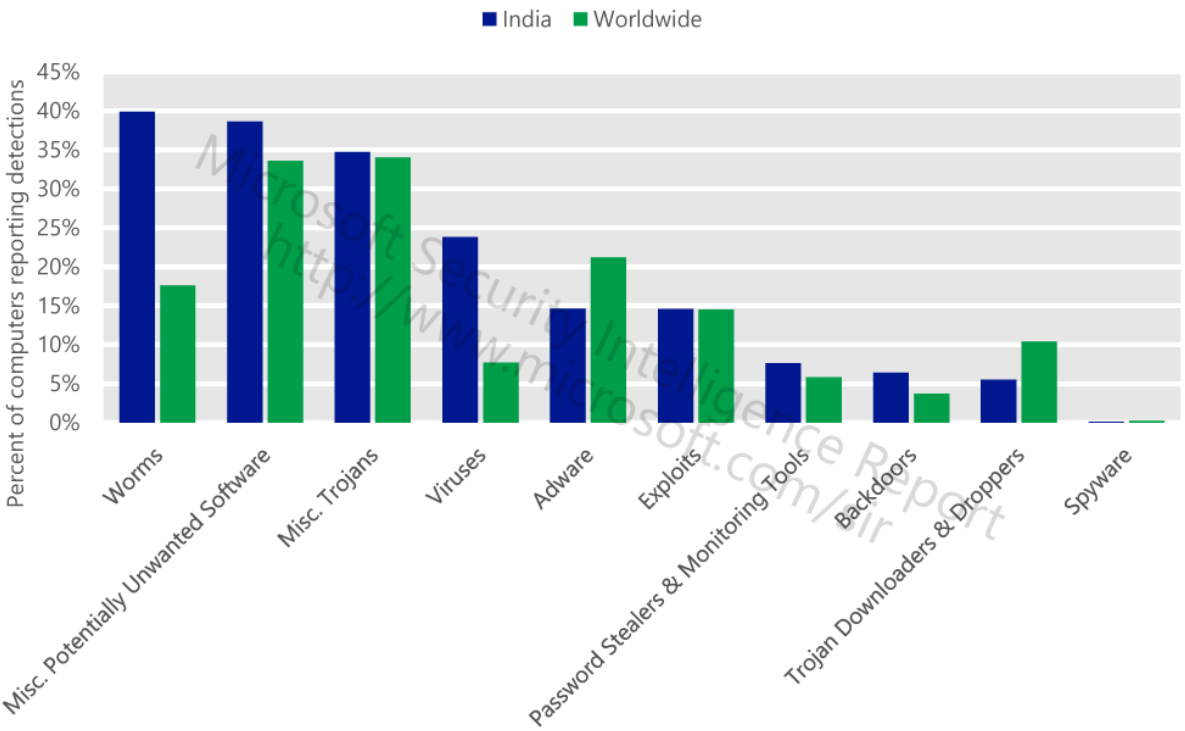


Figure 10. Malware and potentially unwanted software categories in India in 2012, by percentage of computers reporting detections (Microsoft Security Intelligence Report))

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[12] 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[13] 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 and performance. ***[We need to work together to come out with a common acceptable***

[12] 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.
[13] Unique Identification Authority of India - http://uidai.gov.in/

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[14] 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)[15]** is put forward to ensure secure online delivery of e-governance services across various platforms including mobile;
- India's **Mobile governance framework**[16] 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.

[14] 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.

[15] 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.

[16] 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

Cyber security is not just limited to an individual. It extends to organisations and to governments. Its effects are felt at various levels. Cyber security 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, cyber security 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 cyber security 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 cyber security 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 Cyber-security 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 cyber-security 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.

4.4 South Africa – EU priority research areas in Trustworthy ICT[17]

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

1. Research in Cyber Security

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 cyber security 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 cyber security strategies[18]. In South Africa, the focus on cyber security is especially prominent since many geographical regions are incorporated into the global village in an attempt to bridge the digital divide. Cyber security 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 cyber security 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 cyber-security practices that will be sharpened in the future in order to ensure a leading role of Europe and South Africa together in the global cyber security.

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

[17] 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.

[18] "Implementation of a Cyber Security 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 11 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 cyber security 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 Cyber security.

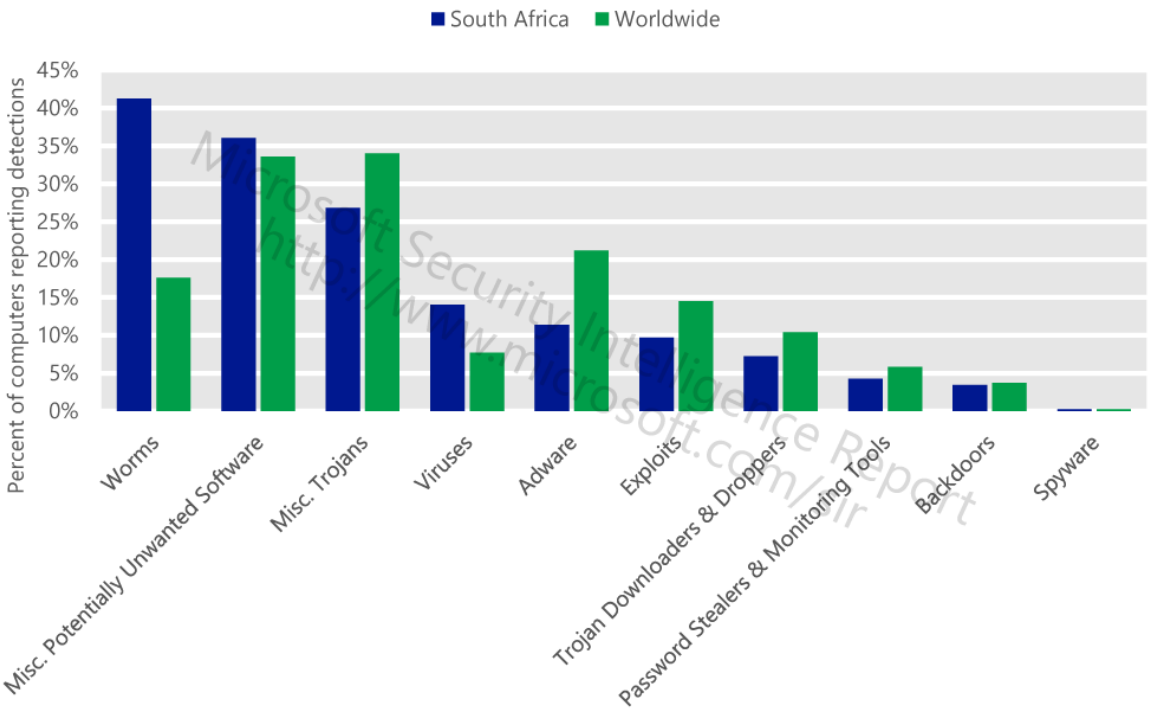


Figure 11. Malware and potentially unwanted software categories in South Africa in 2012, by percentage of computers reporting detections (Microsoft Security Intelligence Report))

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[19] '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[20]. 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 and more accurate with larger sample size. It is, therefore, important to include wider

[19] http://www.bdlive.co.za/business/technology/2013/05/15/cloud-computing-trend-finds-followers-in-sa
[20] http://www.slideshare.net/SamanthaJames_5/cloud-computing-in-south-africa-reality-or-fantasy

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 inFigure 12.

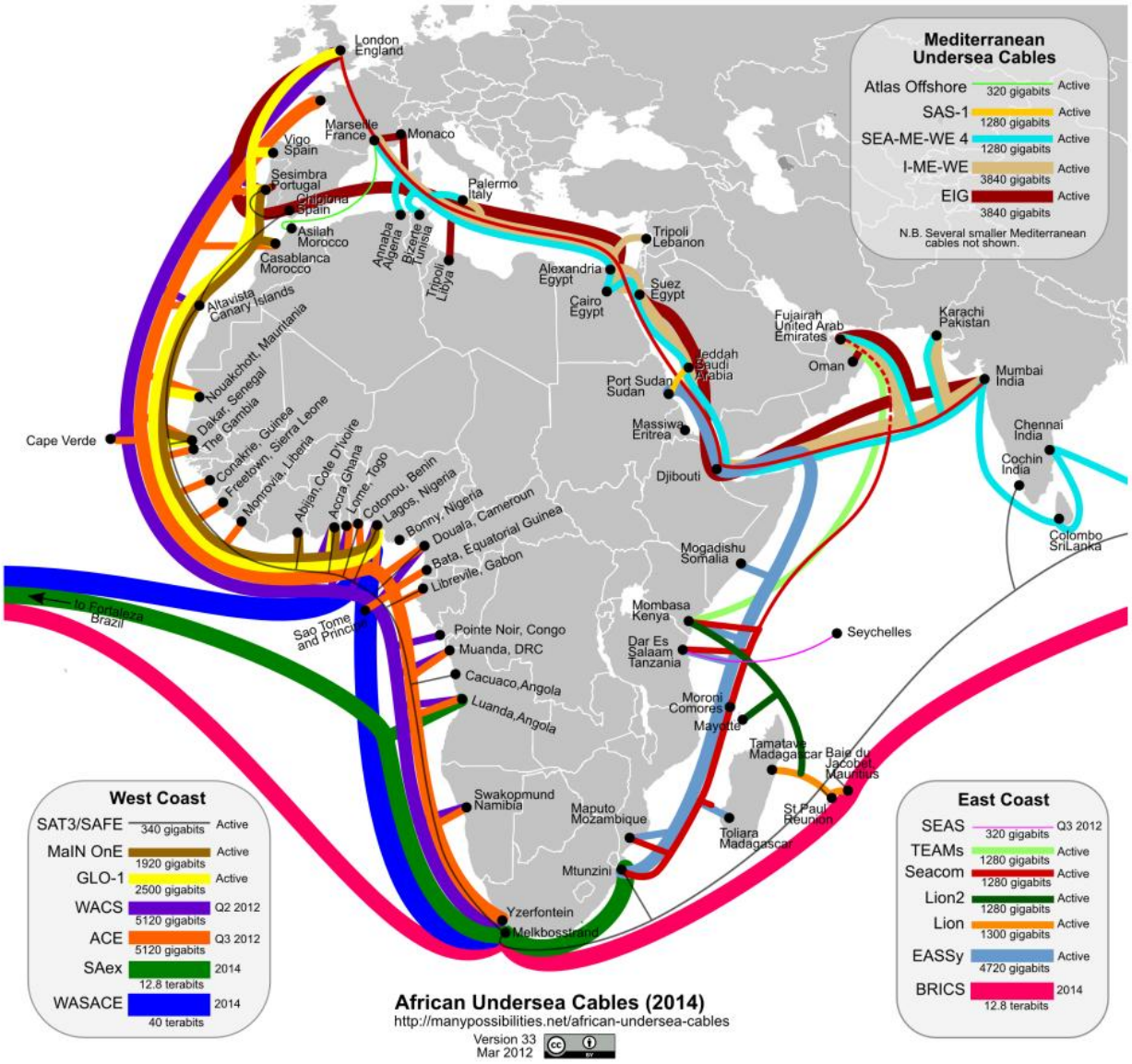


Figure 12. African Undersea Cables in Africa (2014)[21]

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

4.5 Mapping of ranked priority research (Brazil, India, South Africa versus EU)

This section develops a mapping exercise for international cooperation based upon the initial priorities as developed in the sections above. This mapping in Table 5 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 cyber security, identity management, the Future internet security, trust management.	The main India issue, after cyber security, is mobile security.	The main south African issue is cyber security, 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,	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.

governance and provenance aspect.			
Brazil	India	South Africa	EU
Cyber security : resilience of infrastructures, physical and logical infrastructure protection			
International cooperation in Cyber-security: 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	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

international policy elements that need to be developed. They need to be detailed from a multi-national and multi-cultural viewpoint.			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	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	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	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'

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.	authenticated policy enforcement mechanism for the cloud; building Trusted Platform; Privacy preserving processing on the cloud.	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.	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	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	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

	before the cloud could become a major topic of coverage in trust and security	ecosystems and communities to allow them to flourish.	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 cyber-security 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	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[22]. 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

[22] 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.		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.	needs and preferences? The EU FP7 project A4Cloud[23] 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 [1].
Brazil	India	South Africa	EU
Future Internet Security			
Many challenges are introduced according to the necessary	Future Internet: environments that combine sensors (Internet of	"Could Africa become the home of the world's largest botnet or an	Supporting and coordinating research across the continent and

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

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.	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.	unbridled cyber security pandemic?" This is at least a possible scenario given the fast pace of increased broadband (and largely wireless) internet penetration in Africa, where there is currently very low broadband penetration in many areas, high levels of computer illiteracy, sometimes ineffective legislation, and where anti-virus software may be un-affordable or too technically sophisticated for the low-cost devices that are still used. This heterogeneous continent harbours a large socio-techno-digital divide that needs to be accounted for in first-world security solutions since this world is connected to the developed world through the opportunities and challenges of the internet. International, collaborative research can address these challenges by looking at a variety of approaches that require innovative implementation.	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 5. Mapping of EU and BIC countries research agendas in ICT Trust and Security

5 - Conclusions

This deliverable is a report on ranked priority research on future global research challenges in ICT trust and security. It takes into account the workshops and meetings organised by the project and the working groups. Special emphasis is given on the new entrants to the INCO community (via the BIC project) Brazil, India and South Africa, whereby the project initiated, along with IAG and WG members from each country, a working document describing the ranked prioritised ICT Trust and security research topics from their perspectives. In addition, these documents were used during the start-up and establishment phases of External Working Groups (EWG) in each of the BIC countries.

The following contains a summary of the priority research topics for international research in ICT trust and Security for H2020.

Following the description, analysis and the mapping exercises 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 into H2020. Within Table 6, they are ranked into the following six general topics based on the coverage amongst the participating countries and the relevance of the topic within each country.

Topic 1 : Research in Cyber security

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, linkage with privacy mechanisms, 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.

Table 6. Ranked priority research topics

The Horizon 2020 programme will need to take into account the balance between technological dimensions, diversity, interoperability, on the one hand, and usability and flexibility, on the other hand. Table 7 categorises these topics around key challenges of the Future Internet, which will also need to be addressed within Horizon 2020.

Challenge 1. Diversity and interoperability

An ecosystem in the global geography with diversity of cultures and contexts;

Challenge 2. Flexibility and innovation

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

Challenge 3. Trustworthiness

Strengthening the resilience of infrastructure control and crisis management;

Challenge 4. Transparency

Governance and digital control, in Europe and worldwide and digital multi-lateral governance at global scale, neutrality of the entire ecosystem, not just net neutrality;

Challenge 5. Freedom, Openness, Ethics

Principles of human values, flexibility and usability, architecture and usage interrelation and feedback, building together a cyber-ethics;

Challenge 6. 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;

Challenge 7. Trust and Privacy

Digital industrial policy, restoring confidence and privacy, intimacy of cloud computing, repositioning trust infrastructure at the same level as security infrastructure.

Table 7. Key challenges of the Future Internet addressed in H2020

In the BIC Deliverable D3.1 [1], we already listed an initial set of long-term recommendations (2015-2020). As shown in Table 4, the mapping between the ranked priorities and the long-term recommendations may be grouped according the following partitions.

Societal:

- Cyber security : 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:

- Cyber security : 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;
- Appropriate mechanisms for effective INCO, including bi-lateral and multi-lateral cooperation models needed for Cyber security;
- A longer term strategy including coordination, flexibility, and providing for longer durations of continuity is required for maximum impact.

Table 8. Mapping between long term recommendations and priorities.

This research topic prioritisation work will be continued in a number of upcoming internal country External Working Group (EWG) meetings and will be incorporated into the next version of D3.2. Final recommendations report, before being presented at the final International Advisory Group (IAG) meeting.

6 - References

[1] Clarke, J., et. al., BIC Deliverable 4.5 BIC Workshop on success metrics and technical Working Groups (WGs), 22-23rd June 2012, Brussels, Belgium. http://www.bic-trust.eu/files/2013/01/D4.5-BIC-WG-WS-report-V1.pdf

[2] Clarke, J., et. al., BIC Deliverable 4.6 BIC Annual Forum and IAG meeting 2012, 27-28th November 2012, Lisbon, Portugal. http://www.bic-trust.eu/files/2013/01/BIC-Annual-forum-2012-report-Final.pdf

[3] Riguidel, M., et. al., BIC Deliverable 3.1 - Interim recommendations report on future global research challenges in ICT trust and security, May, 2012.

[4] Clarke, J., et. al., BIC Deliverable 4.6, report of the BIC International Workshop on Trustworthiness, Accountability and Forensics in the Cloud (TAFC 2013), 6-7 June, 2013, Malaga, Spain. http://www.bic-trust.eu/files/2013/08/TAFC2013-Workshop-Report.pdf

[5] Threats : Microsoft Security Intelligence Report, Volume 14, December, 2012.

[6] Statistics: Internet usage statistics : http://www.internetworldstats.com/stats.htm

[7] The Global Information Technology Report 2012: Living in a Hyperconnected World, editors: INSEAD, World Economic Forum: www.weforum.org/gitr .

[8] Diego Rafael Canabarro and Thiago Borne, 'Brazil and The Fog of (Cyber)War', http://www.umass.edu/digitalcenter/research/working_papers/13_002_Canabarro-Borne_BrazilandFogofCyberWar.pdf.

[9] Clarke, J., et. al., Report of the BIC – DeitY India Extended Working Group (EWG) Workshop, 21 May, 2013, New Delhi http://www.bic-trust.eu/files/2013/07/BIC-DeitY-EWG-report-final.pdf