D4.4 EU – India Cooperation Workshop

Grant Agreement number: 258655

Project acronym: BIC

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

Funding Scheme: ICT Call 5 FP7

Project co-ordinator: James Clarke
Programme Manager
Waterford Institute of Technology

Tel: +353-71-9166628

Fax: + 353 51 341100

E-mail: jclarke@tssg.org

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

Revision:

Revision [Final]

Project co-funded by the European Commission within the Sixth Framework Programme (2002-2006)		
Dissemination Level		
PU	**Public**	

BUILDING International Cooperation for Trustworthy ICT

European Commission Information Society and Media

EU-India Cooperation and BIC Workshop held 16th December 2011 co-located with eIndia Conference 2011

BIC Partners

TSSG

Waterford Institute of Technology

TECHNISCHE UNIVERSITÄT DARMSTADT

TELECOM ParisTech

Atos

Gandhinagar, Gujarat, India, 16th December 2011

Table of contents

1 Executive Summary

This deliverable details the BIC EU-India events and accomplishments over 2011, that culminated in the BIC EU-India workshop held on 16th December 2011.

In order to build long term sustainable impact, the BIC approach in India (and also for Brazil and South Africa) has systematically utilized a two phased approach.

The first phase is the **operational approach** that involves making specified contacts in the research/policy community and facilitating activities/workshops.

At the same time, we have proactively initiated a second phase where we target a **strategic approach** consisting of meetings/presentations with key unit heads of India's funding organizations and also the policy planners in order for BIC to make long term influence and impact on shaping India's trust and security' planning, whilst at the same time encouraging and strengthening their awareness of Europe's Trust and security outlook.

The second phase, in order to be maximally effective to reach the key audience, took longer than initially anticipated due to the desired scheduling of the BIC cooperation workshop to coincide with India's major ICT eIndia 2011 event in December 2011. An added aspect was the continued difficulty in reaching the key contacts within the India government (e.g. DIT) until very recently. However, the delays were fruitful as the policy contacts worked out and the EU-India workshop was successful.

The following deliverable details the results so far on these two phased approaches with India during the first year of BIC. Significant contacts were made in the research community during the year and in late December 2011. BIC was very successful on both the operational and strategic viewpoints. The first part of the trip specifically targeted the strategic part and consisted of various high level meetings and workshops in New Delhi, culminating in the BIC India – EU Cooperation workshop held 16th Dec. 2011 during eIndia 2011 in Gandhinagar, Gujarat, India.

2 Introduction

During the first year of BIC, pursuing the initial contacts and with further excellent contacts made during the year[1], the BIC partners have discussed with India's trust and security researchers to ascertain the concerns, issues, challenges, and topics of coverage within the country and to examine which of these topics would be mutually beneficial for joint work.

The partners participated to a number of events (including events unfunded by BIC) and drove the discussions on these topics in order to scope how the India researchers approached trust and security in general. We have put together a mapping of the India and EU approaches in order to determine potential topics of coverage that would provide mutual benefit.

- The first main event was a workshop session that BIC organised during the eWorld 2011 conference on 1st August 2011. The BIC project session was designed as an informal session to discuss with participants about the major thrust areas that were important from the India and EU perspectives. This was a successful session and the BIC coordinator Jim Clarke, subsequently presented the findings from this session during eWorld 2011 in a session entitled Information and Management Security held on 3rd August 2011. The presentation and video can be found at http://www.bic-trust.eu/events/eworld-annual-forum/.
- The second event was the BIC India-EU Cooperation Workshop was held on 16th December 2011 during E-India 2011 (held in Gandhinagar, Gujarat, 14-16th December 2011). The event alignment was specifically chosen to capitalize that many prominent Indian ICT researchers/policymakers in attendance at India's largest ICT event. The well attended BIC workshop contained presentations from the BIC partners and also from researchers from India. The presentations were followed with a panel of questions and answers from the audience, which included government, industry, academic and research participants.

The approach taken has been to present the trust and security perspectives from the EU and to compile the perspectives from India and then to map them into joint collaboration activities of mutual benefit. The following sections contain a summary of each of the countries perspectives and then a potential mapping for joint collaboration topics of EU and India in trust and security.

3 India perspective on trust and security research

3.1 Background

The fast emergence of the information and communication technology (ICT) sector in India economy has placed this country on the digital world scene since the past fifteen years. The Indian ICT sector has grown at a remarkable rate and the flow of information

[1] based on contacts received from the European Commission, Europe's India delegation officer and other projects in which BIC partners were invited as working group and advisory board members

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

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

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

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

3.2 How is Trust and Security research funded in India

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

The Cyber Laws & eSecurity Group, as shown in Figure 1**,** contains a number of different programmes:

- Cyber Security strategy [1] - A cyber security strategy has been outlined by DIT to address the strategic objectives for securing country's cyber space and is being implemented through the following major initiatives: Security Policy, Compliance and Assurance; Security Incident Early Warning & Response; Security training skills/competence development & user end awareness; Security R&D for Securing the Infrastructure, meeting the domain specific needs and enabling technologies; and Security Promotion & Publicity.
- Cyber Laws strategy [2] - Provides legal recognition to electronic documents and a framework to support e-filing and e-commerce transactions and also provides a legal framework to mitigate, check cyber crimes.
- Cyber Security R&D strategy [3] – promotes research & development activities through grant-in-aid support to recognized autonomous R&D organizations and academic institutions proposing to undertake time-bound projects in the thrust areas identified.

The closest to Unit F5 Trust and Security within DG-INFSO of the European Commission [17] would be a combination between the Cyber Security strategy and Cyber Security R&D groups, probably more so towards the latter. The DIT mainly funds research and academic institutions. There are other programmes that may also touch upon some of the other topic areas covered in the EU including one dealing with judicial matters in relation to Cyber space, the Cyber Appellate Tribunal (CAT[5]); Indian Computer Emergency Response Team (ICERT[6]), the nation's referral agency of the Indian Community for responding to computer security incidents as and when they occur; and Controller Of Certifying Authorities (CCA[7]), provided for by the Information Technology Act, 2000 [8] as the governing authority which licenses and regulates the workings of Certifying Authorities [9], who issue digital signature certificates for electronic authentication of users.

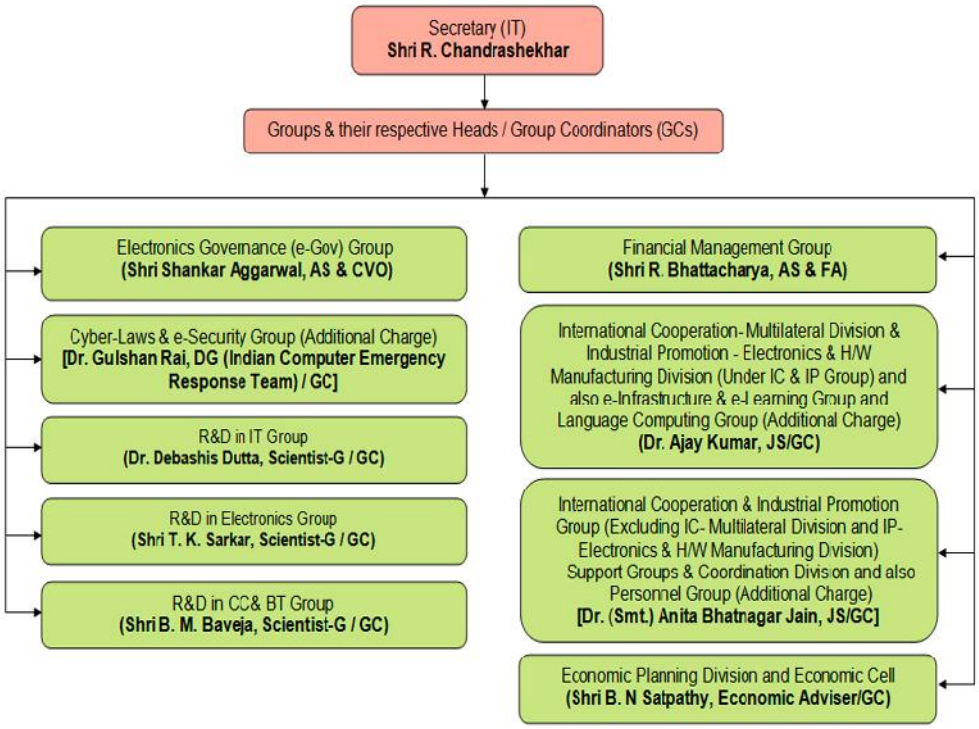


Fig. 1. DIT Groups and their respective Heads/Group coordinators [4]

With regards to International cooperation and how it links to Trust and Security, there is an International cooperation Directorate that works very closely with the Directorate under which the Cyber Security and eSecurity group belong. There are a number of departments related to international cooperation and the most appropriate one for Trust and security research would be the Department of International Cooperation & Industrial Promotion, Bilateral Trade Division [10]. There are already a number of FP7 projects engaged in EU – India cooperation (e.g. ERNET India connectivity with European Research Network – GEANT) and these are detailed at [10].

How funding or R&D projects in Cyber Security Works

Department of Information Technology (DIT) invites R&D project proposals in Cyber Security area. Cyber Security R&D initiative of DIT in an open call fashion that is aimed at promotion of basic research, technology demonstration, proof-of-concept along with indigenous development of technology in the area of Cyber Security [11].

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

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

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

Monitoring tools for network and system security, (vi) Enterprise forensics and (vii) Mobile forensics.

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

3.3 Key research focus areas

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

- The increasing complexity of IT systems and networks, which will present mounting security challenges for both the providers and consumers.
- The evolving nature of the telecommunications infrastructure, as the traditional phone system and IT networks converge into a more unified architecture.
- The expanding mobile and wireless connectivity to individual devices, computers and networks, which increases their exposure to attack. In hybrid or all-wireless network environments, the traditional defensive approach of securing the perimeter is not effective because it is increasingly difficult to determine the physical and logical boundaries of networks.
- The increasing interconnectivity and accessibility of (and consequently, risk to) computer-based systems that are critical to the country's economy, including supply chain management systems, financial sector networks, and distributed control systems for factories and utilities.
- The breadth and increasingly global nature of the IT supply chain, which will increase opportunities for subversion from attackers within and outside the country.

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

The policy, articulated by the DIT Cyber Security R&D Group, lays emphasis across the spectrum - Basic research, Technology demonstration and Proof-of concept and R&D test bed projects [12]. It stems from the consideration that indigenous R&D is an essential component of national Information strategy in order to:

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

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

The areas of near to medium term public-funded Information Security research in India under the aegis of the Cyber Security R&D department within the Department of Information Technology (DIT) are [13]:

A. Cryptography and Cryptanalysis

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

B. Network and Systems Security

- Virtual Private Network Security solutions;
- Security of key internet protocols (Ipv4 to Ipv6), Domain Name System (DNS) and Border Gateway Protocol (BGP), routers, servers;
- Security of wireless devices, protocols and networks;
- OS Security and trusted OS;
- Automatic generation of test suites, safe programming languages;
- XML security.

C. Security Architectures

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

D. Vulnerability and Assurance

D.1 Vulnerability Detection and Analysis

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

D.2. Assurance Technologies

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

E. Monitoring, Surveillance and Forensics

E.1. Intrusion Detection

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

- proactive Intrusion Detection Systems;
- Intrusion detection for high speed networks.

E.2. Content and Traffic Analysis

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

E.3. Computer Forensics

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

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

- The Indian approach to trust and security in ICT is functional, rather than conceptual. The main concentration is on the 'plumbing' or 'nuts and bolts' rather than a focus on the concepts behind the design of the systems.
- Indian research in 'Trust and Security' areas focuses predominantly on Indian competitiveness, technological edge, import substitution, functional areas, networks, devices and architectures, rather than having a 'service to end user' perspective in its articulation.
- Trust, privacy and security in India are not sufficiently appreciated from the perspective of citizens' rights, benefits for business and society's entitlements, although there is a strong community led by the Data Security Council of India advocating strong privacy and data protection as a lever for economic development of India through global integration of practices and standards conforming to various legal regimes and promoting India as a global 'secure' place to conduct business [14]. The published mission of the Data Security Council of India is "To create trustworthiness of Indian companies as global sourcing service providers, and to assure clients worldwide that India is a secure destination for outsourcing where privacy and protection of customer data are enshrined in the global best practices followed by the industry." [15]
- There is a serious concern with the security, integrity and reliability of hardware, especially when highly reliant on imports in India.
- Unique Identification (UID) project: How to guarantee protection of the citizen's rights, security, privacy in the context of the mammoth Unique Identification (UID) project, which is currently in the roll out phase.
- The increasing complexity of IT systems and networks and expanding mobile and wireless connectivity present mounting security challenges, which substantially increases their exposure to attack.
- The level of the Indian cryptography research is very high (e.g. the famous "Primes is in P" result showing that there is an elegant deterministic polynomial time algorithm for primality testing of integers secure OS standards for smart cards at IIT Kanpur); theoretical and practical aspects of cryptography, number theory, computational complexity.

- The level of the Indian mathematics research is well recognized in applied mathematics: data mining and machine learning, formal approaches to security.
- CERT to be a premier reference in Asia Pacific Region (New Zealand, Vietnam, Australia, Korea…).
- Data and Intellectual Property (IP) vision needs to be improved to become a secure country for data and IP. IP risks due to employee turnover.
- Cyber forensics for tracking attackers and enforcement purposes, protection against the social network of hacker groups, and establishing their Modus Operandi; Promoting awareness in cyber-security among students through ethical hacking contest.
- Multilinguism issues in trust and security: language-independent information dissemination using NFC. Multilingual systems are a serious challenge in India.
- Cybercrime (virus in email, trojan in webpage, fraud in ecommerce transactions, e-robbery in e-banking transaction, identity theft in credit card payment).
- Terrorism on physical telecom infrastructures (fixed or wireless telecommunication network operations) and cyber-terrorism with unlimited resources and motivation or cyber warfare with rogue nations.
- Development of trust models for cloud computing: client authenticated policy enforcement mechanism for the cloud; building Trusted Platform; Privacy preserving processing on the cloud. However, there was a strong opinion from the researchers that broadband coverage issues within India should be addressed in a more serious way before the cloud could become a major topic of coverage in trust and security.
- Security of Mobile telecoms; and building trust for Mobile transactions.
- Cryptographic protocols between Payment System Provider, Deposits, Payment and Authorization) for micro-payment is highly suited for India.
- E-governance, information sharing, surveillance and analysis: to foster collaboration between federal, state, and local agencies as well as the private sector.

List of ongoing projects

The following is a list of ongoing projects funded by the DIT Cyber Security R&D department [16]:

1. Project title: Development of test bed for Information Security skill development using Virtual Training Environment (VTE)

Project objectives: To design and simulate various scenario based problems and solutions using virtual training environment systems with associated lab manuals for Incident handling, Intrusion analysis, Perimeter security, Hardening of systems, Network Security testing, Cyber Forensics.

Project coordinator: Alok tripathi, sr. design engineer, DOEACC Society, Gorakhpur, gkp.alok@gmail.com

2. Project title: Development of Person Authentication System based on Speaker Verification in Uncontrolled Environment

Project Coordinator: Dr. S. R. Mahadeva Prasanna, Associate Professor, Indian Institute of Technology, Guwahati-781039, Assam, prasanna@iitg.ernet.in

Project objectives: 1) Development of speaker verification database in multilingual, multi-sensor and uncontrolled environment; 2) Research and development of a speaker

verification system for speech data collected from uncontrolled environment; 3) Development of person authentication system using speech and one of the non-biometric features like PIN targeted to phone banking.

3. Project title: Cyber Forensics & Digital Analysis Centre in short to be known as "Cyber Centre"

Project coordinator: Shri B. Ramani, CDAC, Thiru and Shri Tomin.J. Thachankary, IPS, IGP, SCRB, Kerala Police Thiruvananthapuram, gkp.alok@gmail.com

Project Objectives: 1) To establish a State of Art Cyber Forensics and Digital Analysis Centre in Kerala for the benefit of Law Enforcement Agencies and other Stake holders; 2) To develop Human "Resources to handle matters related to Cyber" Forensics from among various stake holders; 3) To educate even the students in basics of Cyber Forensics as a preventive measure against cyber crimes; 4) To conduct real case analysis and give expert opinion in crime cases, civil disputes to facilitate investigation and to assist Courts; 5) To reduce the burden on the Cyber Forensics Resources Centre of C-DAC Tvpm in order to give more time to the Scientists of C-DAC, Tvpm for Research and Development.

4. Project title: CYBER & HI-TECH CRIME INVESTIGATION and training

Project coordinator: Director, CBI Academy Ghaziabad, CBI Academy, Ghaziabad, Gorakhpur- 273010, gkp.alok@gmail.com

Project Objectives: To impart training to cyber crime investigators, forensic examiners and Trainers and potential Trainers of the Police Training Institutions in the country in the fields of - (i) Cyber Crime Investigation and (ii) Cyber Forensics.

4 EU perspective on trust and security research

4.1 Background

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

In operational terms, the European Commission's Directorate General (DG) Information Society and Media (DG-INFSO), through its **"Trust and Security"** unit F5 [17], through whom the BIC project is funded, is entrusted with supporting and coordinating research across the continent and through international cooperation. Research priorities in this domain are strongly related to the development of the Future Internet and target:

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

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

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

4.2 How is Trust and Security research funded in the EU

The most recent of the European Commission’s multi-annual calls for proposals has been Call 8 of ICT Work programme 2011 – 2-12, which included specifically a topic on Trustworthy ICT [18].

Under Framework Programme 7 (2007 – 2013), the European Commission’s most recent call including trustworthy ICT is call 8, which includes an Objective ICT-2011.1.4 entitled Trustworthy ICT, as part of the challenge 1 of the ICT Work Programme 2011-2012. The objective is a trustworthy Information Society based on an ecosystem of digital communication, data processing and service provisioning infrastructures, with trustworthiness in its design, as well as respect for human and societal values and cultures. Projects must ensure strong interplay with legal, social and economic research

in view of development of a techno-legal system that is usable, socially accepted and economically viable [19].

4.3 Key research focus areas

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

Heterogeneous networked, service and computing environments

- ***Trustworthy (meta) architectures and protocols*** for scalability and interoperability, taking account of heterogeneity of domains, partitions, compartments, capabilities and environments in ecosystems and underlying infrastructures; architectural standards, including meta-level specifications, for conformity, emergency and security policy management.
- ***A trustworthy polymorphic future internet*** with strong physical security in balance with privacy; federated, seamless, transparent and user-friendly security of the edge networks in smart ecosystems, ensuring interoperability throughout the heterogeneous landscape of access networks.
- ***Virtualisation and other techniques*** to provide protection, assurance and integrity in complex, high-demand critical services; and security in the presence of scarce resources, and in legal domains with different priorities. Trustworthy global computing with contextual security and secure smart services in the cloud.
- ***Metrics and tools for quantitative security*** **assessment** and predictive security in complex environments and for composition and evaluation of large scale systems.
- ***Enabling technologies*****,** such as declarative languages, biometry, technology for certification and accreditation or cryptography for Trustworthy ICT.

Trust, e-Identity and Privacy management infrastructures

- Development of ***trust architectures, protocols and models*** for trust assurance, including measures and rating models, and services and devices to enable trust assessment (e.g. by claims on identity, reputation, recommendation, frequentation, voting), to delegate trust and partial trust; and for trust instrumentation and high-level tools at the end-user stage (cognitive and learning instrumentation for trust, profiling services and communities).
- Protocols for ***privacy infrastructures*** enabling multi-identity and tools to check privacy assurance and enable un-observability and un-linkability through search engines or social networks. Advancement of privacy at the hardware level.
- Interoperable or federated ***management of identity claims*** integrating flexible user-centric privacy, accountability, non-repudiation, traceability as well as the right to oblivion at the design level. Technologies and standardisation for use of multiple authentication devices, applicable to a diversity of services and ecosystems, and providing auditing, reporting and access control.

Data policy, governance and socio-economic ecosystems

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

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

Networking and Coordination activities

- Support for networking, road-mapping, coordination and awareness raising of research and its results in Trustworthy ICT.
- Priority will be given to (i) stimulating and organising the interplay between technology development and legal, social and economic research through multi-disciplinary research communities; (ii) promoting standards, certification and best practices; (iii) coordination of national RTD activities.

Expected impact:

- Improved European industrial competitiveness in markets of trustworthy ICT, by: facilitating economic conditions for wide take-up of results; offering clear business opportunities and consumer choice in usable innovative technologies; and increased awareness of the potential and relevance of trustworthy ICT.
- Adequate support to users to make informed decisions on the trustworthiness of ICT.
- Increased confidence in the use of ICT by EU citizens and businesses. Increased usability and societal acceptance of ICT through understanding of legal and societal consequences.
- Demonstrable improvement (i) of the trustworthiness of increasingly large scale heterogeneous networks and systems and (ii) in protecting against and handling of network threats and attacks and the reduction of security incidents.
- Significant contribution to the development of trustworthy European infrastructures and frameworks for network services; improved interoperability and support to standardisation. Demonstrable usability and societal acceptance of proposed handling of information and privacy.
- Improved coordination and integration of research activities in Europe or internationally.

4.4 Mapping of India and EU approaches to Trust and Security

In this section, we have analysed the India and EU approaches to trust and security in order to establish a number of potential areas for India –EU cooperation that would take into account the varying different perspectives. The following table contains the mapping of the two countries perspectives and chapter 5 contains a list of potential themes that are derived from the analysis of this table.

India approach to trust and security	EU approach to trust and security
• 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.	• The EU approach is to examine (or make attempts) to examine the in depth concepts and horizontal aspects for trust, privacy and security e.g. empowering the users to gain control over trust, security and privacy issues. Emphasising the horizontal aspects of trust and security in ICT, by highlighting multi-disciplinary research and the relevance of aspects like usability, societal acceptance and economic and legal viability of the research results.
• Indian research in 'Trust and Security' areas 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.	• Enabling technologies for security and trustworthiness of ICT that guarantees rights, addresses security, trust and protect the privacy and personal data of the users and enables participative governance
• Security, privacy and trust in India are not sufficiently appreciated from the perspective of citizens' rights, benefits for business and society's entitlements (although there is a strong community advocating the need for this!)	• Concept of 'Privacy by Design' embedding privacy proactively into technology, thereby ensuring full privacy and data protection and 'Identity Management'
• There is a serious concern with the security, integrity and reliability of hardware.	• Supporting and coordinating research across the continent and through international cooperation, by prioritising the development of the 'Future Internet'
• 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.	• Balancing between the right to anonymity (privacy) and the societal imperative of making personal data available
• The increasing complexity of IT systems and networks and expanding wireless connectivity present mounting security challenges which substantially increases their exposure to attack. • The level of the Indian cryptography research is very high (e.g. the famous "Primes is in P" result showing that there is an elegant deterministic	• 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. • Increasing the leadership of the European cryptography skill which is recognized at the international level.

India approach to trust and security	EU approach to trust and security
polynomial time algorithm for primality testing of integers secure os standards for smart cards at IIT Kanpur); theoretical and practical aspects of cryptography, number theory, computational complexity.	
• The level of the Indian mathematics research is recognized in applied mathematics: data mining and machine learning, formal approaches to security.	• Significant work ongoing in formal methods for trust and security engineering.
• CERT to be a premier reference in Asia Pacific Region (New Zealand, Vietnam, Australia, Korea…).	• Ensuring the CERT in Europe is tracking attacks and send out periodic advisories and generate statistics and trends in cyber-attacks.
• Data and Intellectual Property vision needs to be improved to become a secure country for data and IP. IP risks due to employee turnover.	• Intellectual Property: developing standards for the industry and creating awareness among stakeholders about security and privacy issues.
• Tracking attackers, and the social network of hacker groups, and establishing their Modus Operandi; Promoting awareness in cyber-security among students through ethical hacking contest.	• Europe has strict legislation on the rights and obligations with digital data. The fight against fraud and cyber-crime is implemented in each country with a relatively good efficiency. The behavior of the attackers is reduced to playing hide and seek with the police on the internet. This niche is more and more narrow and difficult. The attacker status is different in some emerging countries (Asia, Africa, South America) where the legislation is not yet ready or the means to fight against cyber-criminality are not yet deployed.
• Multilinguism issues in security: language-independent information dissemination using NFC. Multilingual systems are a serious challenge in India.	• The diversity of languages and scripts, as a security issue, is underestimated in Europe.
• Cybercrime (virus in email, trojan in webpage, fraud in ecommerce transaction , e-robbery in e-banking transaction, identity theft in credit card payment)	• Malicious attacks: in Europe, for researchers, on top worry list is data misuse followed by network-oriented issues such as malicious traffic attacks or data integrity on the network itself. Industry experts put

India approach to trust and security	EU approach to trust and security
	breaches of trust within companies and misuse of personal information – for example through Facebook or e-banking – as their number one internet security concern. Vulnerabilities in emerging Cloud environments due to reduced ownership of resources and data is also a concern.
• 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.	• 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.
• Development of Trust models for Cloud Computing: client authenticated policy enforcement mechanism for the cloud; building Trusted Platform; Privacy preserving processing on the cloud. • Security of Mobile telecom; building trust for Mobile transactions.	• 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.
• Cryptographic protocols between Payment System Provider, Deposits, Payment and Authorization) for micro-payment is highly suited for India. • • •	• There is a lack of mechanisms to upgrade cryptographic algorithms and protocols in the mobile telecom industry for the existing baseline (GSM, 3G) infrastructures. Cryptography-based solutions for micropayment face tremendous deployment challenges. They significantly change payment ecosystem processes (legal implications, new devices and processes).
• E-governance, information sharing, surveillance and analysis: to foster collaboration between federal, state, and local agencies as well as the private sector.	• The deployment of government services available to the citizens (G2C) in a convenient, efficient and transparent manner is raising serious scalability and privacy issues.

5 Conclusions

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

5.1 Theme 1: Digital ecosystem trustworthiness

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

- **CERT**: A cooperation to enhance the security ICT realm through proactive action and competent collaboration is required for the current exploitation of the ICT infrastructures (internet, mobile telecoms). International cooperation must be enhanced in this area in order to create awareness about DDOS, BOTS, phishing, etc. Annex 1 contains details of the Indian Computer Emergency Response Team: statistics from 2010.
- **Protection against malware:** when there is a heavy reliance on imported systems as in India: approaches to influence the manufacturing process and to guarantee protection at source.

5.2 Theme 2: Trust & Privacy

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

- **Language-independent Security:** security usability is a major challenge for any culture and any country: return of experience from outside could be beneficial for both continents. India and Europe are continents where several languages and several scripts. Usability for alarms, alerts, warnings is an important factor for improving the understanding of the mechanisms and awareness of security. A cooperation could benefit to both continents.
- **Trust, Security and Privacy in mobile environments:** mobile connectivity that accommodates the heterogeneity and failure-proneness of both devices and network to gel with issues such as broadband and sparse coverage in India. Also, the need for usable security in the mobile environment e.g. the simple elements of data integrity and security that lets people “trust” the devices to do banking and other activities given that the mobile platform is the sole/primary platform for many users in India.
- **Identity management (eg. India’s UID, EU’s privacy protecting ID systems):** biometrics – Europe and India could work together on low cost, less power intensive equipment providing the required accuracy. Authentication, built upon the strong work in India and EU, could mutually improve potential future solutions.
- **Strong societal push in both EU and India:** Putting citizens in control of their data and how can technologies provide this control to citizens? Forging strong link between

social scientists and technologists. How to deal with conflicts between the "right to info", "access to personal data", "updating the data" and right-to anonymity (be forgotten).

- **Balance between strong security tools and efficiency and effectiveness -** Security with flexibility; building cost effective, tailor made, indigenous security products that compete for export market.

5.3 Theme 3: Global Framework and international alignment

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

- **Convergence of physical and cyber worlds:** To ensure the security of society either in the physical world or the cyber-world requires coming together of all stakeholders with a collaborative effort. We need to share experiences on building secure knowledge society.
- **Appropriate regulations**: Policy makers must find appropriate regulations in order to coordinate efforts from different stakeholders to try to develop a roadmap of cyber-security practices that will be sharpened in the future in order to ensure a leading role of Europe and India together in the global digital economy.
- **International Data Exchange for Cybersecurity:** Secure data exchange and sharing for analysis and CERTs working well together.
- **Attackers and Hackers**: There is a need to work together on addressing the international data exchange and sharing of information and intelligence on cyber-attacks for a free flow of the information in a secure and reliable manner. To collectively fight against cyber-threats an organized response is requested to understand the emerging threats and identify solutions and create a roadmap of actionable activity schemes.
- **Intellectual Property**: Cooperation to create a platform for promoting sharing of knowledge about information security and foster the community.
- **Risk management approaches to trust and security:** Looking at the economics of security and privacy. Trade-offs between risk and security: what does it cost to society?

5.4 Theme 4: Engineering and Scientific domains

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

- **Cryptography -** Cooperation with the centre of Mathematics and Cryptography (the Indian Statistical Institute (Kolkata), ITT (Kanpur, Chennai, Kharagpur) for stream ciphers, hash functions, provable security, elliptic curve pairing theory, secure multi-party computations, steganalysis, side channel cryptanalysis; E-passport.
- **Cyber Forensics –** RTD in software tools for use in forensic investigations in today's ICT environments (cloud computing, mobile etc.). This is a topic of importance in India where they would like to work with the EU researchers that was raised at the BIC workshop.

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

5.5 Theme 5: International Cooperation on Cyber-security

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

The growth of a digital ubiquitous, ecosystem has pushed innovation of enormous value for the global economy and society. The meta-system construction with software, hardware, and digital data has created a critical infrastructure upon which the smooth functioning of essential sectors depends. While providing societal benefits, this exciting opportunity has also produced a major and growing complex of risks for all countries around the world.

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

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

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

Already links have been established by BIC with the International cooperation directorate at the DIT and there is an upcoming meeting of High Level Working Group being held in Q1 2012, which would hopefully lead to actions on further mechanisms for joint India – EU cooperation on a number of topics, including ICT Trust and Security.

References

[1] DIT, Cyber Security strategy http://www.mit.gov.in/content/cyber-security-strategy
[2] DIT, Cyber laws strategy, http://www.mit.gov.in/content/cyber-laws
[3] DIT, Cyber Security R&D strategy, http://www.mit.gov.in/content/cyber-security-r-d
[4] DIT, Organisation chart 2/5, http://www.mit.gov.in/content/organization-chart
[5] DIT, Cyber Appellate Tribunal (CAT), http://www.mit.gov.in/content/crat-dpl-other
[6] DIT, Indian Computer Emergency Response Team (ICERT), http://www.mit.gov.in/content/icert-dpl-other
[7] DIT, Controller Of Certifying Authorities (CCA), http://www.mit.gov.in/content/cca-dpl-other
[8] Information Technology Act, 2000, http://cca.gov.in/rw/pages/informationtechnologyact2000.en.do
[9] Certifying Authorities, http://cca.gov.in/rw/pages/becoming_ca.en.do
[10] Department of International Cooperation & Industrial Promotion, Bilateral Trade Division, http://www.mit.gov.in/content/europe

[11] DIT, Cyber Security R & D Call for proposals http://www.mit.gov.in/sites/upload_files/dit/files/CyberSecurity.pdf
[12] DIT, Cyber Security R & D mission statement http://www.mit.gov.in/content/cyber-security-r-d
[13] DIT, Cyber Security R & D mission statement Thrust areas http://www.mit.gov.in/content/thrust-areas
[14] Data Security Council of India http://www.dsci.in/

[15] Data Security Council of India mission statement http://www.dsci.in/taxonomypage/1

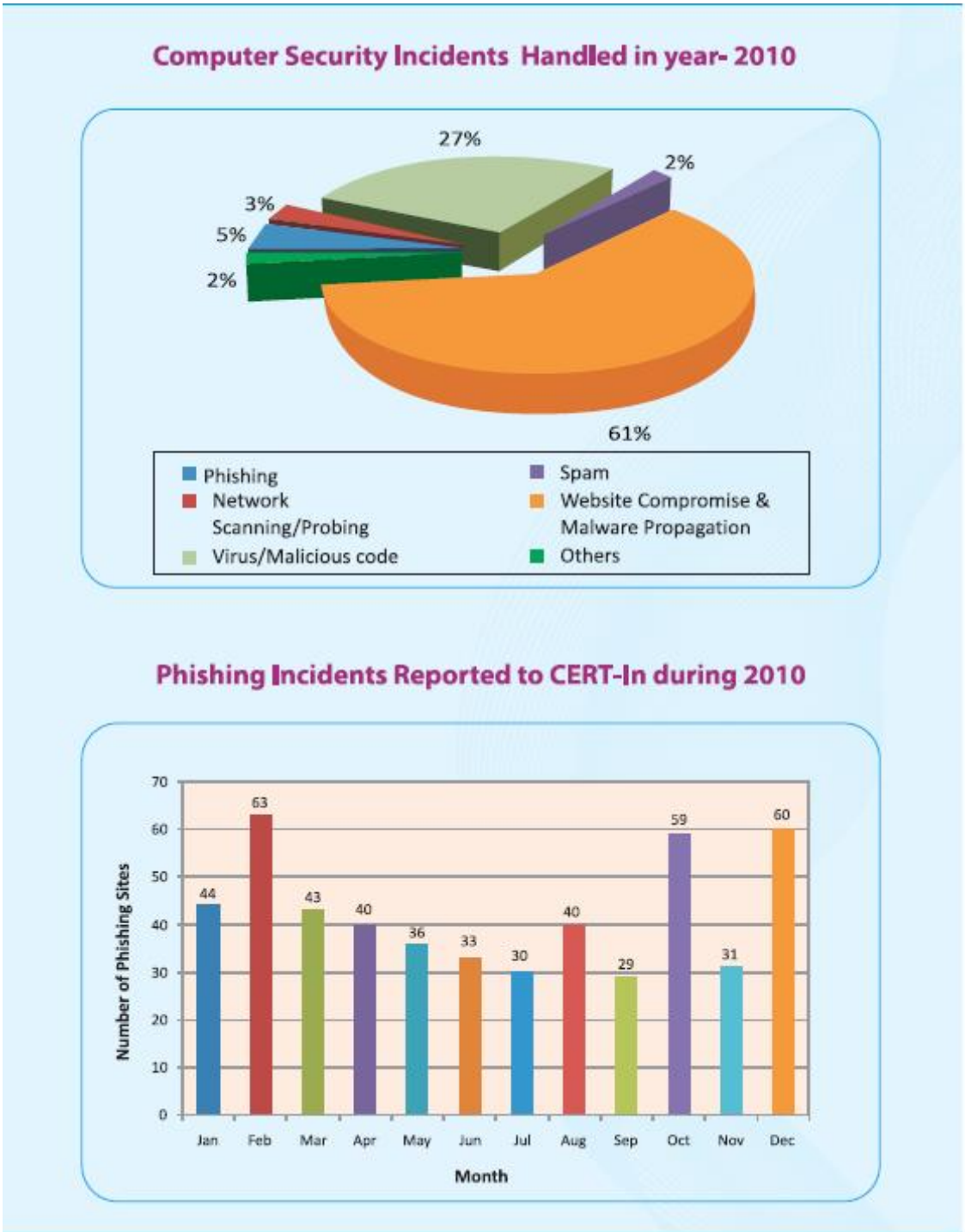
[16] DIT, Cyber Security R & D List of ongoing projects http://www.mit.gov.in/content/list-ongoing-projects

[17] DG-INFSO Unit F5 Trust and Security http://cordis.europa.eu/fp7/ict/security/home_en.html

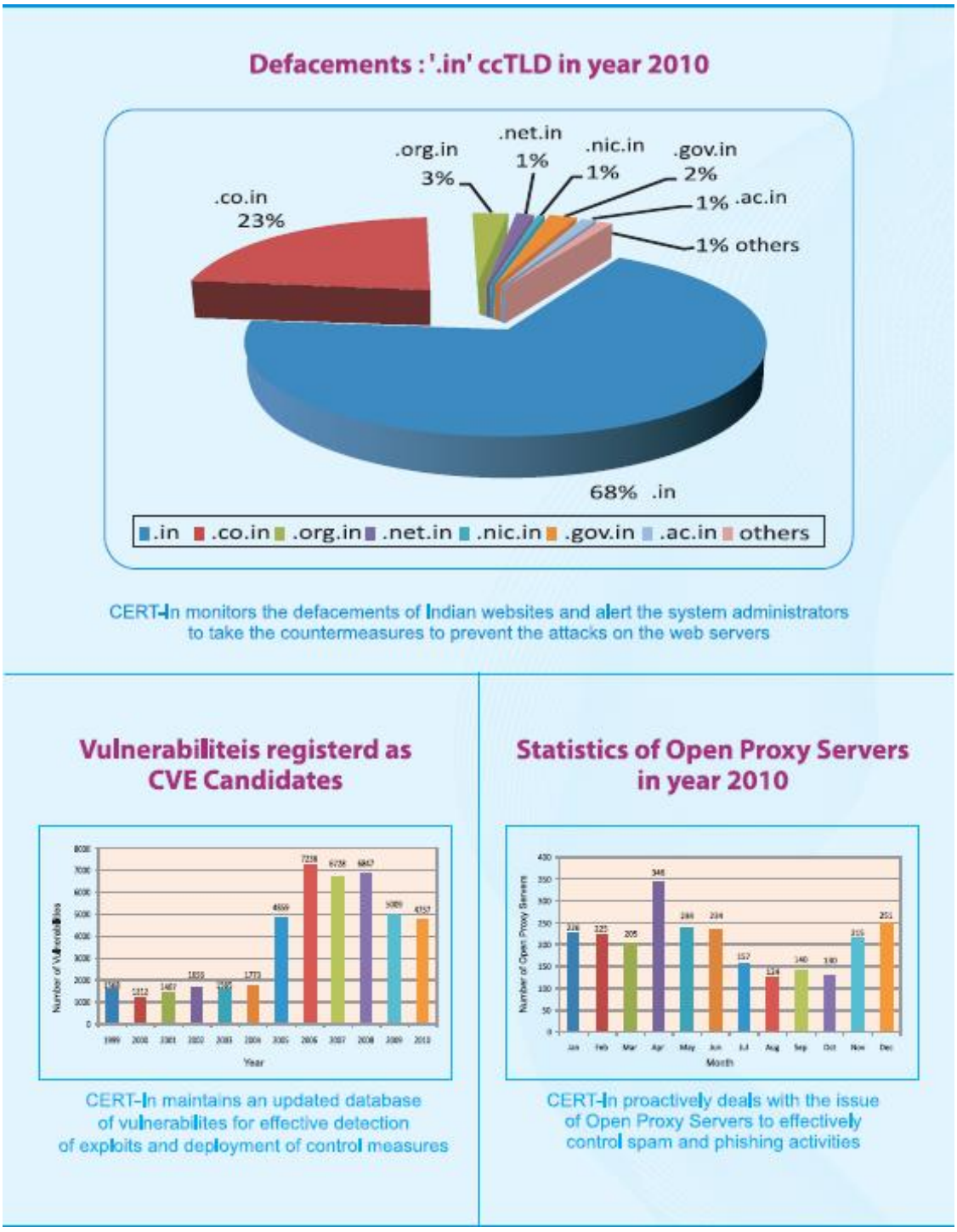
[18] Work Programme 2011 – 2012 Announcement of FP7, Call 8 http://cordis.europa.eu/fp7/ict/

[19] Announcement of FP7, Call 8 http://cordis.europa.eu/fp7/ict/security/fp7-calls-trustworthy_en.html

Annex 1. India CERT statistics for 2010



Indian Computer Emergency Response Team: statistics 2010



Indian Computer Emergency Response Team: statistics 2010