A strategic approach for Building International Cooperation (BIC) in Cyber Security: *BIC success in India*

Thought paper for CyFy conference, 14-15th October, 2013, The Oberoi, New Delhi, India

28 September 2013

James Clarke[1]

Abhishek Sharma[2]

[1] Waterford Institute of Technology, Ireland

[2] Abhishek Sharma, BIC International Advisory Group (IAG) member, Co-founder, MD & CEO, Beyond Evolution Tech Solution Pvt. Ltd., India

This project is supported within the portfolio of the European Commission's DG-CNECT Unit H.4, Trust and Security, and has received funding by European Commission's Seventh Framework ICT Programme under grant number 25258655 for the period January 2011 to December 2013.

Introduction

In today's world, it is one of the most cherished dreams of the people across the globe to have a Trusted ICT environment where they can feel confident using the technology without any fear of loss of privacy, wealth or any personal assets that are linked to technology assisted transactions in any form. Cyber security, which is at the core of such a "Trusted ICT" environment, is a borderless global phenomenon impacting every nation.

The purpose of the European Commission funded BIC coordination action project (http://www.bic-trust.eu/) is to foster cooperation between the EU and the international programme agencies and researchers in India, Brazil and South Africa within the focus areas of Trustworthy ICT, including trust, privacy and security, in order to:
(a) Understand the activities and planning of the target countries; and
(b) Carry out a mapping of the European Commission's planning to them, such that a common technical and policy alignment is viable.

Accordingly the objectives of the BIC's "Strategic approach for Building International Cooperation (BIC) in Cyber Security" are:

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

In addition to scoping technical research themes for INCO, the project is also working with the communities in a coordinating role in reflecting on a longer term strategy for international cooperation. The project held a recent workshop looking at topics for potential INCO projects and advancing the international cooperation strategy in June 2013 and during this two day workshop [1], a special session was held on this strategy. This paper reflects on the results from this workshop and proposes a potential approach to follow based on the findings.

The Strategic INCO approach

In order to examine the challenge of moving from a bi-lateral to a multi-lateral approach (Figure 1), the project held an earlier workshop in June 2012 [2] bringing together a majority of the projects engaged in international cooperation to enable the following outcomes:

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

In addition to BIC, a wealth of experience was represented from the following international cooperation projects: IST Africa, EuroAfrica-P8, FEED, AUS-ACCESS4EU, PACE-Net, EU – India Spirit, Synchroniser, Euro-IndiaGrid2, OpenChina-ICT, FIRST, FORESTA, PAERIP, SEACOOP, EuroAfrica-P8 and AMERICAS. A full report of the BIC workshop can be found at [2].

These projects gave their insights on their experiences and suggestions for improvement and the main point was agreement that it is a very good idea to move towards a more multi-lateral strategic position. However, in the discussions, it wasn't very clear how this strategy shift could occur within the current mechanisms that focus bi-laterally on seven (7) distinct regions.

In order to address this further, the BIC project are examining how the combination of their International Advisory Group and supporting working groups could assist in a move towards a more multi-lateral strategic approach.

The majority of the current INCO mechanisms support regional bi-lateral activities as shown in Figure 1. While this regional approach may work for higher level themes, the main difficulty arises when a particular research topic, for example, cyber security, needs to be addressed globally and multi-laterally amongst many regions and the bi-lateral approach is not suited for this type of longer term strategic activity. Therefore, the BIC project is examining the feasibility of a more strategic approach based on multi-lateral partnerships as shown in Figure1.

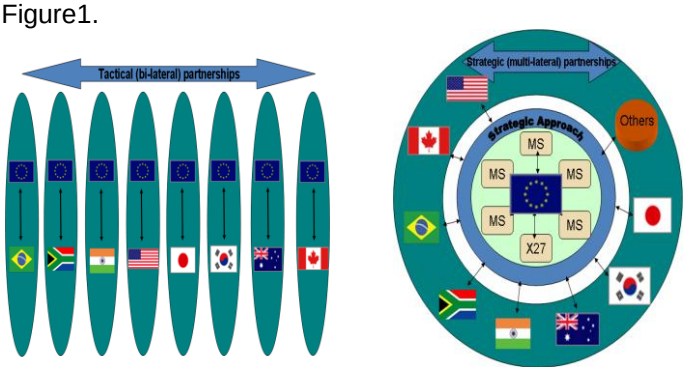

Figure 1 – Tactical (bi-lateral) approach *versus* Strategic (multi-lateral) approach

BIC International Advisory Group (IAG)

The BIC project has established an international advisory group (IAG) with the following terms of reference.

The IAG will be the forum bringing together the countries representatives in a more strategic way;

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

The IAG has representation from all the participant countries from both the researcher communities and programme management (funding agencies). The IAG is there to suggest and formulate the policies, processes and mechanisms to achieve international cooperation in the area of the ICT Trust and Security community. Three independent working groups, WG1, WG2 & WG3 with specific objectives as defined in the BIC WG Terms of Reference [3], have been formed comprising specialists from different countries and different specializations. The areas and scope of the three BIC working groups are the following:

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

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

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

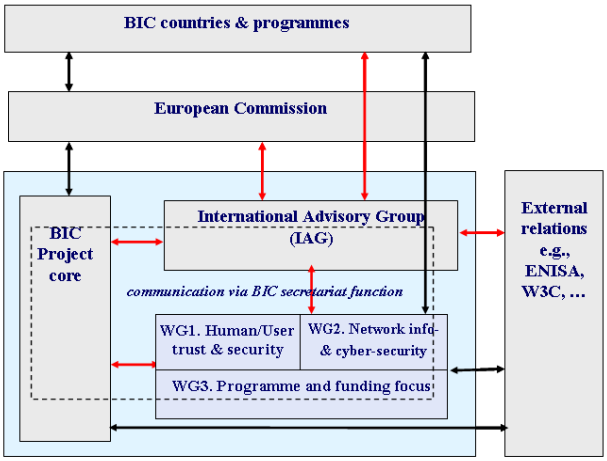

Figure 2 – Overall structure of BIC

Indeed, as shown in Figure 2, these WGs form the backbone of the project; however, they alone would not be enough to take the entire project forward to its logical conclusion. They would, therefore, need to be supported by additional Groups and Sub-Groups in a structured manner as shown in figure 3, at the management and functional level with defined focus area, roles and responsibilities.

Since the nature of the project requires interactions amongst all participant countries to share the information, resources, etc., the approach for the formal interactions, flow of information and smoothness of actions, it becomes natural that the groups and sub groups working for the project work closely with each other. Accordingly at international management level, it requires a change in approach from the existing bi-lateral approach i.e. EU-India, EU- Brazil, EU- SA, U.S, Japan etc to multi-lateral approach where each participating country develops a formal system for direct multi-lateral communication and interacts with each other besides interacting centrally as well. Of course, the existence and role of a central body is essential for ensuring that the focus of the projects are not digressed and there is proper coordination amongst all adhering to the core principles and objectives of the project.

A possible multi-lateral structure is outlined here n Figure 3.

a. Core Working Group (CWG); based on the current BIC IAG and supporting WGs as shown in Figure 3.
b. Extended Working Groups (EWGs) – specific for each participating country as shown in Figure 3.
c. Special Function Groups – operating under EWGs as specialists at functional level.

Note: Although not envisaged as part of the original BIC project structure as seen in Figure 2, the BIC countries, with India in the lead place, have already undertaken to set up in-country EWGs and these will be discussed in more detail in the next section of the paper.

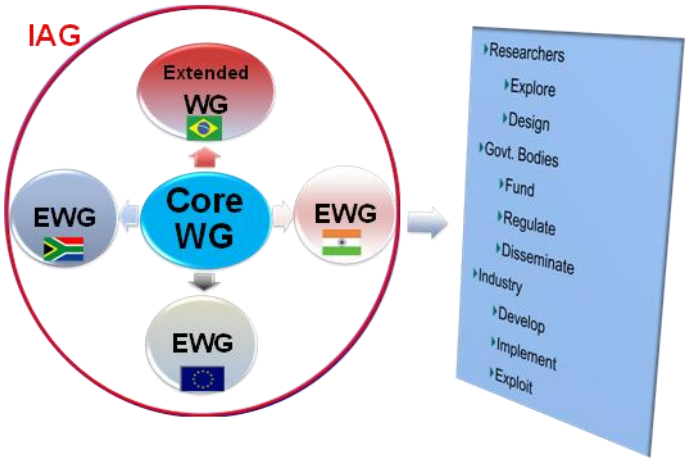

Figure 3 – BIC IAG/Working Groups structure

India – EU cooperation

Throughout the BIC project, Indian researchers and the Government of India as part of the IAG of BIC have been very active in formulating a strategic approach for cooperation and also promoting key research themes in Trustworthy ICT of mutual benefit for India – EU collaboration. In fact, the Indian community have activated the very first External Working Group of BIC and the launch and kick off meeting was held on Tuesday, 21st May 2013 in New Delhi in the conference hall of the Department of Electronics and Information Technology (DeitY) of the Government of India [4].

The prioritised topic of research within Cyber Security topped the list of topics during the launch workshop. A number of recent items form the backdrop to the interest in collaboration within cyber security research, including (but not limited to):

- 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*[3], was published.
  - 9th May, 2013: India's National Cyber Security Policy was approved by the Government of India[4];
  - 2nd July, 2013. India's National Cyber Security Policy[5] was formally notified.

In addition, the strategic 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 has established Network Information Security (NIS) Public Private Platform (PPP), whose objectives are to discuss standardisation needs and economic, legal and technological incentives that could be defined at EU, national or sectorial level. 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.

Within BIC, the following research challenges of mutual benefit 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.
- 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. Moreover, 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 [5].
- International Data Exchange for cyber security: Secure data exchange and sharing for analysis and CERTs working well together [6]. 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

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

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

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

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 [7].
- 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 [8].
- 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;
- Cyber 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 4 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 [9].

Conclusions

The building of international cooperation is difficult when using a bi-lateral approach as it takes significant time for all of the parties to come together to try to align their activities and priorities. Therefore, it is even more difficult for a multi-lateral approach when building a longer term strategy as proposed within this paper. The BIC project has proposed a strategy and India has taken a lead role as an exemplar, being the first country to establish an organised External Working Group according to this strategy.

The BIC project is going to bring this topic to the next level at the upcoming BIC Annual Forum/IAG meeting being held on 7th November 2013 in Vilnius, Lithuania, being held as part of the major ICT 2013, launch of Horizon 2020 Research programme. The strategic approach for international cooperation will be a main topic of the terms of reference and agenda for the IAG meeting [10].

This India – EU achievement clearly addresses the long term strategy of BIC as it is pretty clear these structures can continue long after the conclusion of BIC and shows the strong commitment of the research community and government of India and their desire to cooperate with EU researchers in the upcoming Horizon 2020 programme. The in-depth and committed views of participants also strongly suggest that H2020 programme needs to set up another BIC - like programme that can seamlessly continue the objectives accomplished so far and the achievements of the BIC carry forward its International Cooperation objectives that have strongly emerged during the progress of the BIC project.

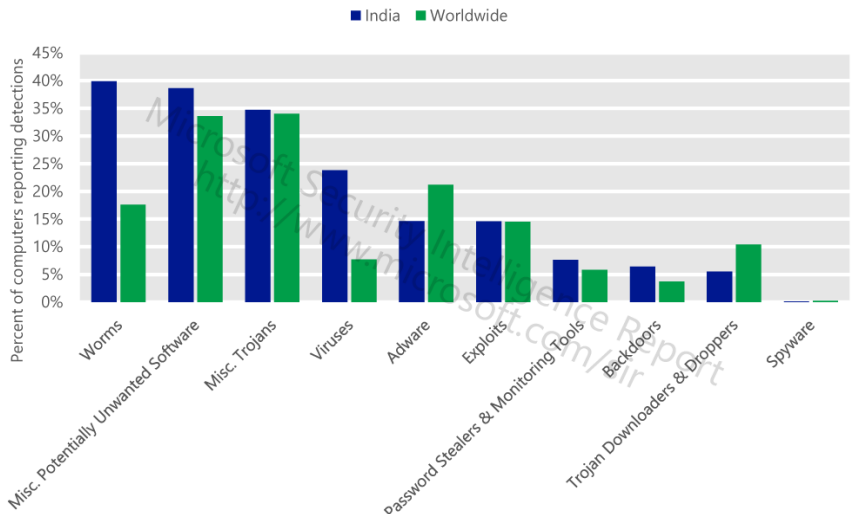

Figure 4. Malware and potentially unwanted software categories in India in 2012, by percentage of computers reporting detections (Microsoft Security Intelligence Report))

Acknowledgments

The BIC project [11] is supported within the portfolio of the European Commission's DG-CNECT Unit H.4, Trust and Security [12], and has received funding by European Commission's Seventh Framework ICT Programme under grant number 25258655 for the period January 2011 to December 2013.

A considerable amount of local organisation for the BIC EWG launch event in May 2013 as reported in this paper took place over a number of months in India and the EU, especially spearheaded by paper co-author and BIC International Advisory Group members, Mr. Abhishek Sharma, CEO of Beyond Evolution Technologies, Dr. Manmohan Chaturvedi, Professor Ansal University and the strong interactions and support of BIC IAG member, Dr. Gulshan Rai, the Director General of Indian Computer Emergency Response Team (CERT-In), Department of Electronics & IT (DeitY), Ministry of Communications & IT of the Government of India. The project also appreciates Professor M. P. Gupta, Chair of the Information Systems and Centre for Excellence in E-government at the Indian Institute of Technology (IIT) Delhi, who has agreed to take on the role of steering the EWG of India.

The organisers are very appreciative of all of the attendees from Government, Industry and Academics for taking their time to attend and contribute.

The organisers are also very appreciative of the strong interest and support shown by the European Commission, Delegation of the European Union to India, including Dr. Philippe de Taxis du Poët and Dr. Klaus Pendl.

References

[1] BIC Workshop June 2013 site http://www.bic-trust.eu/files/2013/08/TAFC2013-Workshop-Report.pdf

[2] Clarke, J., et. al., BIC Workshop on Cross domain coordination of International Cooperation and technical themes in Trustworthy ICT and INCO. Online report - http://www.bic-trust.eu/files/2012/04/BIC_D4.5_Report-of-Workshop.pdf

[3] BIC Deliverable D2.3 - Interim report of the Working groups activities (restricted).

[4] 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

[5] Interventions of Dr. Jaijit Bhattacharya, Director, Government Advisory, Hewlett Packard, BIC EWG meeting, 21 May, 2013, BIC EWG launch workshop, 21 May, 2013.

[6] Interventions of Dr. Gulshan Rai, Director General of Indian Computer Emergency Response Team (CERT-In), DeitY, Ministry of Communications & IT of the Government of India. BIC EWG launch workshop, 21 May, 2013.

[7], [8] Interventions of Dr. N Vijayaditya, Ex CCA and DG, NIC, Govt. Of India, BIC EWG launch workshop, 21 May, 2013.

[9] Interventions of Dr. Jaijit Bhattacharya, Director, Government Advisory, Hewlett Packard, BIC EWG meeting, 21 May, 2013, BIC EWG launch workshop, 21 May, 2013.

[10] http://www.bic-trust.eu/2013/09/06/bic-iag-annual-forum-2013/

[11] BIC Web site http://www.bic-trust.eu/

[12] DG CNECT Unit H.4 web site http://cordis.europa.eu/fp7/ict/security/

About the Authors

Abhishek Sharma is founder, MD & CEO of Beyond Evolution Tech Solutions Pvt Ltd(beTS). Abhishek has built beTS from scratch developing many mobile application and Solutions offering niche Utility VAS as ASP to large mobile users through many large Telcos like Vodafone, BSNL, MTNL, Idea, Airtel etc in India and abroad. Prior to founding beTS, Abhishek has worked for Indian Air Force for about 22 yrs and then for large corporate in India and abroad such as Programme Manager, GSM Backhaul/ Microwave Services, Tata Telecom, India; Country Head – Telecom SBU at TCS/ Tata Infotech, India; MD at Globacom Cellular, Nigeria etc where he managed large ICT Projects & Operations such as Radar, Telecom NW, BSS, OSS etc. Abhishek is also a renowned consultant on Mobile VAS, Telecom Network, Radar Data Systems & Avionics. Abhishek is B.E. in Electronics & Telecommunications, M.Tech Computer Sc (IISc) & M.B.A. in Marketing.

James Clarke has been working for the Waterford Institute of Technology (WIT) in the Telecommunications Software and Systems Group (TSSG), since February 2005. Prior to joining WIT-TSSG, Mr. Clarke worked at LAKE Communications in Ireland for eight years and Grumman Corporation in the United States for eight years. Since January 2011, Mr. Clarke has been the project coordinator of a European Framework Program 7 Co-ordination action entitled 'BIC', which stands for Building International Cooperation for Trustworthy ICT: Security, Privacy and Trust in Global Networks & Services. Previous to this, Mr. Clarke coordinated the successful FP7 INCO-Trust project. More information can be found at **http://www.tssg.org/about/people/james-clarke/.**