Telecommunication Development Sector

Regional Preparatory Meeting for the Americas Region for WTDC-10
Santa Marta, Colombia, 9 - 11 September 2009

Document RPM-AMS09/48-E
11 September 2009

Original: English

For information

SOURCE	**Telecommunication Development Bureau**
TITLE	**ITU-IMPACT Initiative**

Contact point: Name/Organization/Entity: M. Maniewicz, Chief, BDT/POL
Phone number: +41 22 730 5421
Email: mario.maniewicz@itu.int

INTERNATIONAL TELECOMMUNICATION UNION

Telecommunication
Development Bureau

TELEFAX

Place des Nations
CH-1211 Geneva 20
Switzerland

Telephone +41 22 730 51 11
Telefax Gr3: +41 22 733 72 56
Gr4: +41 22 730 65 00

Date: Time: Page 1/7 Ref: BDT/POL/CYB DM -136

To: To Heads of Administrations of all ITU Member States Fax:
cc: Mr. Mohd Noor Amin, Chairman, Management Board, IMPACT

For your reply:

Contact: Marco Obiso, ICT Applications and Cybersecurity Advisor, BDT/POL

E-Mail: cybmail@itu.int

Fax: +41 22 730 5484 Tel: +41 22 730 6760

Subject: Deployment of Cybersecurity Capabilities - IMPACT Global Response Centre

Dear Sir,

I am writing to inform your Administration that discussions took place during the International Telecommunication Union (ITU) Council 2008 and the Internet Governance Forum, on the International Multilateral Partnership Against Cyber Threats (IMPACT) initiative.

ITU and IMPACT formally entered into a Memorandum of Understanding in which IMPACT's new state-of-the-art global headquarters in Cyberjaya, Malaysia, will effectively become the physical home of the ITU's Global Cybersecurity Agenda.

Launched in 2007 by ITU Secretary-General, Dr Hamadoun I. Touré, the ITU Global Cybersecurity Agenda (GCA) is a framework for international cooperation aimed at enhancing confidence and security in the information society.

The close synergies between the five work areas of the Global Cybersecurity Agenda and the services and infrastructure provided by IMPACT made a joint-partnership a logical step in the global fight against cyber threats, cybercrime and other misuses of Information and Communication Technologies.

ITU, through its Telecommunication Development Sector, has gained significant experience in facilitating the establishment of national strategies for cybersecurity and critical information infrastructure protection, including capacity development, and can draw on an extensive network of leading cybersecurity authorities.

In order to respond properly to the five areas identified by the GCA, as well as to follow up on ITU's work to assist countries in developing cybersecurity capabilities, ITU is working with IMPACT to make the following resources available to ITU Member States:

- Global Response Centre
- Training and Skills Development

- Centre for Security Assurance and Research
- Centre for Policy and International Cooperation

The first service that will be made available is the Global Response Centre (GRC).

The GRC is designed to be the foremost cyber threat resource centre in the world. Working with leading partners including academia and governments, the Centre will provide the global community with a real-time aggregated early warning system. This ‘Network Early Warning System’ (NEWS) will help member countries identify cyber threats early on and provide critical guidance on what measures to take to mitigate them.

The GRC will provide ITU Member States with access to specialized tools and systems, including the recently-developed ‘Electronically Secure Collaborative Application Platform for Experts’ (ESCAPE). ESCAPE is an electronic tool that enables authorized cyber-experts across different countries to pool resources and collaborate with each other remotely, yet within a secure and trusted environment. By pooling resources and expertise from many different countries at short notice, ESCAPE will enable individual nations and the global community to respond immediately to cyber-threats, especially during crisis situations.

In addition to the GRC offerings, IMPACT offers scholarship grants to eligible developing country Member States for training courses delivered through the SANS Institute, United States. The training focuses on building a pool of resources that can later share the knowledge acquired with others, to build national capacity and expertise in the field of cybersecurity.

Within the framework of the preparation to the World Telecommunication Development Conference 2010, Regional Preparatory Meetings (RPMs) will take place in 2009 and 2010 in all ITU regions, and are expected to contribute to shaping the objectives and the strategies for a balanced regional development of telecommunication and ICT. During these Meetings, special sessions will be dedicated to the ITU-IMPACT collaboration in order to present the initiative and related activities to the ITU Member States.

Attached is additional information on the GRC. Information can also be found online at www.itu.int/osg/csd/cybersecurity/gca/impact/   The GRC services can be tailored to meet individual Member State requirements.

To become involved in the activities mentioned above, please respond to this letter, highlighting the specific area and services that your country is interested in.

We welcome you to the coalition and look forward to your valuable inputs on how to properly assist ITU Member States.

Thank you.

Yours faithfully,

Sami Al Basheer Al Morshid
Director

Annex: Technical Note: Global Response Centre

Technical Note

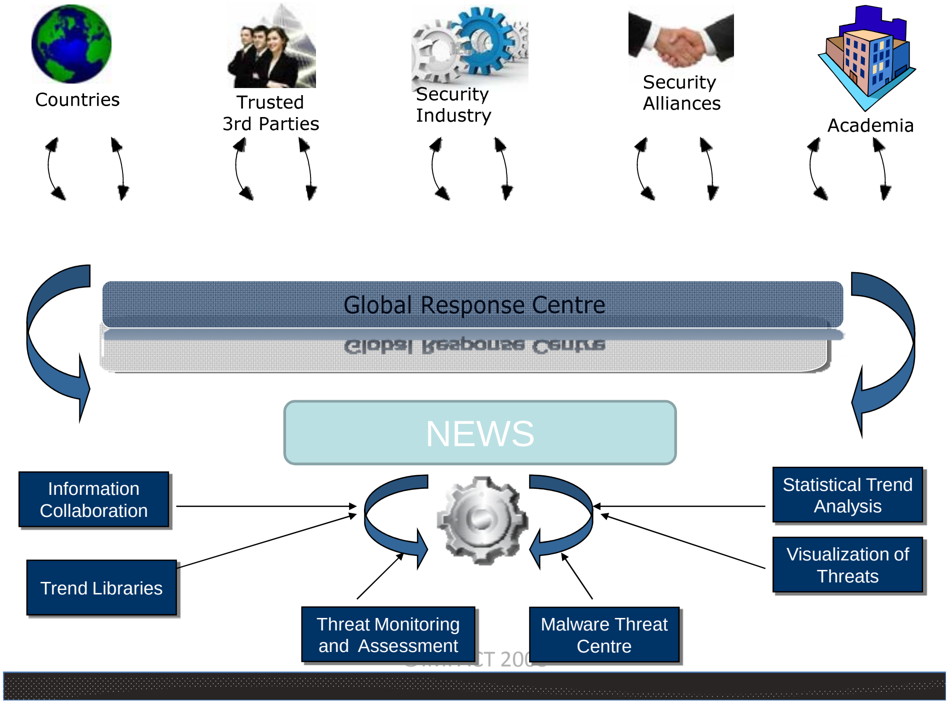
GLOBAL RESPONSE CENTRE

INTRODUCTION

IMPACT's Global Response Centre (GRC) acts as the foremost cyber threat resource centre for the global community. It provides emergency response to facilitate identification of cyber threats and sharing of resources to assist IMPACT members. The two prime highlights of GRC are NEWS (*Network Early Warning System*) and ESCAPE (*Electronically secure collaboration application platform for experts*).

NEWS (Network Early Warning System)

Working with leading partners in the industry, academia, and governments (current partners include Symantec Corporation, Kaspersky Labs, F-Secure, Trend Micro, SANS institute etc.), the GRC will provide the global community with real time early warning system - NEWS.



Thus, NEWS would serve as a vehicle of information collaboration as well as information dissemination of up to date information on security trends. NEWS provides features like:

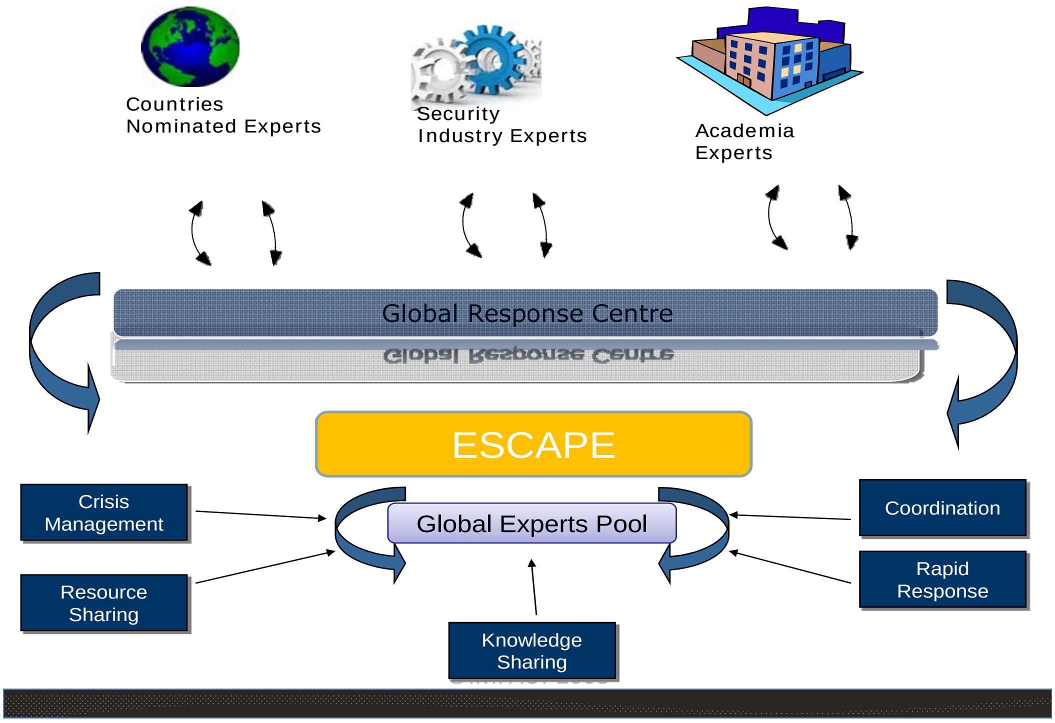
1. Real time threat monitoring and assessment: Whereby member countries can see the global severity threat level and solutions to mitigate the threat.

2. Statistical cyber threat trend analysis: where by member countries can see minute view of current cyber trends and threats around the world, presented as a collection of easy to read charts, graphs, maps and tables.

3. Malware threat centre: Where by members can upload malware and the get feedback on the full technical details of the malware analysis.

ESCAPE (Electronically Secure Collaboration Application Platform For Experts)

In addition to NEWS, IMPACT will provide its member countries with ESCAPE. ESCAPE is a unique electronic tool that enables authorized cyber experts across the different countries to pool resources and remotely collaborate with each other in a secure and trusted environment.



This system features a comprehensive and growing database of key resources around the world – including IT experts, empowered persons (government regularity officials), and other trusted bodies (CERTS), who can be called in to assist during a crisis. Thus, members can rapidly create a response team to deal with almost any emerging cyber threat. With a state of the art team collaboration platform and access to experts from government, academia and private industry, IMPACT provides an unrivaled platform for global emergency response.

Introductory Package

All member countries are welcomed aboard with the GRC's introductory package. This entitles them to have access to NEWS and ESCAPE. IMPACT's Global Network Early Warning System (NEWS) would provide IMPACT members an up to the minute view of cyber threats around the world. These threats are drawn on data from dozens of public and private security feeds and presented as a collection of easy to read charts, graphs, maps and tables. NEWS would allow the members to seek the sources of attacks emerging round the globe; identify the current cyber threats and cyber security breakouts.

Introductory package also provides the member countries to discover and connect with other cyber security professionals throughout the IMPACT network via ESCAPE. By applying enterprise social networking techniques to IMPACT member countries, IMPACT allows members to draw on the wealth of expertise within the IMPACT community. The introductory package provides up to five multiple logins to the ESCAPE and ability to add local cyber security experts to the IMPACTS expert community. With this package the member countries can escalate their security problems to the global IMPACT experts, who would provide assistance and right solutions. Furthermore, ESCAPE would provide periodic security news, reports, and ability to upload a malware for inspection and analysis by the IMPACT experts to its member countries.

For introductory package members would dedicate a Computer Security Incident response team member to provide assistance as and when required.

Because all the introductory member's hardware and software are hosted by IMPACT's Global Response Centre in Malaysia, this membership is ideal for countries that desire a higher level of presence and recognition without making an investment in local infrastructure.

IMPACT – Introductory Functionality Offered

Description	Introductory
Global Response Centre	
• **Access to ESCAPE**	**From 1 Public IP Address**
• **Ability to have access to NEWS data and visualization**	√
• **Maximum number of ESCAPE portal accounts**	**5**
• **Ability to invite local experts to the IMPACT expert community**	√
• **Ability to escalate incidents to the IMPACT expert community**	√
• **Ability to upload malware for IMPACT analysis**	√
• **Ability to receive periodic security news**	√
• **Ability to receive periodic security reports (Generic)**	√
• **Ability to subscribe to ESCAPE's content**	√
• **Minimum number of Computer Security Incident Response Team members nominated**	**1**
Training & Skill Development	
• **Training on ESCAPE**	√
• **Training on NEWS**	√

Standard Package

Member countries that choose to play a more prominent role in IMPACT may elect to opt for the standard membership package. On top of the introductory package the standard package member enjoy much more feature and services of GRC.

The standard package provides features like hundred multiple logins to the ESCAPE, access to IMPACT's online library on knowledge base, and full retrieval of technical details of any malware uploaded. Standard member would be able to receive periodic security reports customized and tailored to their own requirements (region specific, or industry specific like oil and gas, finance, etc.)

IMPACT will provide its Standard members with email as well as telephonic notification of security emergencies and furthermore, assistance via GRC analyst and consultant. Standard members also have the ability to raise service requests, access online meetings, sponsor private groups, create and access private discussion forums, create and manage limited access teams, etc.

To provide assistance as and when required the member country would dedicate up to five computer Security Incident response team member to member countries on Standard package. Standard members have a choice to opt for local hosting or using IMPACT's Global Response Centre in Malaysia hardware facilitates.

IMPACT –Standard Functionality Offered

Description	Standard
Global Response Centre	
• **Access to ESCAPE**	**From 1 Public IP Address**
• **Ability to create multiple logins to access the ESCAPE**	√
• **Ability to have access to NEWS data and visualization**	√
• **Maximum number of ESCAPE portal accounts**	**100**
• **Ability to invite local experts to the IMPACT expert community**	√
• **Ability to escalate incidents to the IMPACT expert community**	√
• **Ability to upload malware for IMPACT analysis**	√
• **Ability to retrieve full technical details of malware analysis**	√
• **Ability to receive periodic security news**	√
• **Ability to receive periodic security reports (Generic)**	√
• **Ability to receive periodic security reports (Customised)**	√
• **Email notification of security emergency**	√
• **Telephonic notification of security emergency**	√
• **Access to GRC analyst and consultant**	√
• **Access to IMPACT Online Library and Knowledge Base**	√
• **Access to online meeting**	√
• **Ability to subscribe to ESCAPE's content**	√
• **Ability to raise Service Request**	√
• **Ability to create Localized Team (Team Management)**	√

• **Minimum number of Computer Security Incident Response Team members nominated**	**5**
•	
Training & Skill Development	
• **Training on ESCAPE**	√
• **Training on NEWS**	√

Mr. Sami Al Basheer Al Morshid
Director
Telecommunication Development Bureau
International Telecommunication Union
Place des Nations
CH-1211Geneva 20
Switzerland

Ref : BDT/POL/CYB DM-136

Subject: Deployment of Cybersecurity capabilities - IMPACT Global Response Center

Dear Director,

In reference to your letter on the aforementioned subject, we would like to thank you for the opportunity given to ____________ to be involved in the ITU-IMPACT initiative.

In this regard, we are pleased to confirm our interest in joining the coalition and have the opportunity to receive concrete services and facilities within the framework of the ITU Global Cybersecurity Agenda and support the ITU Development Sector in its efforts toward achieving Cybersecurity.

In consideration for ____________ being a Partner and obtaining access to the services of the GRC and the facilities of IMPACT, ____________is interested in the following areas:

- Global Response Center (NEWS,ESCAPE)
- Training and skills development
- Centre for Security Assurance and Research
- Centre for Policy and International Cooperation

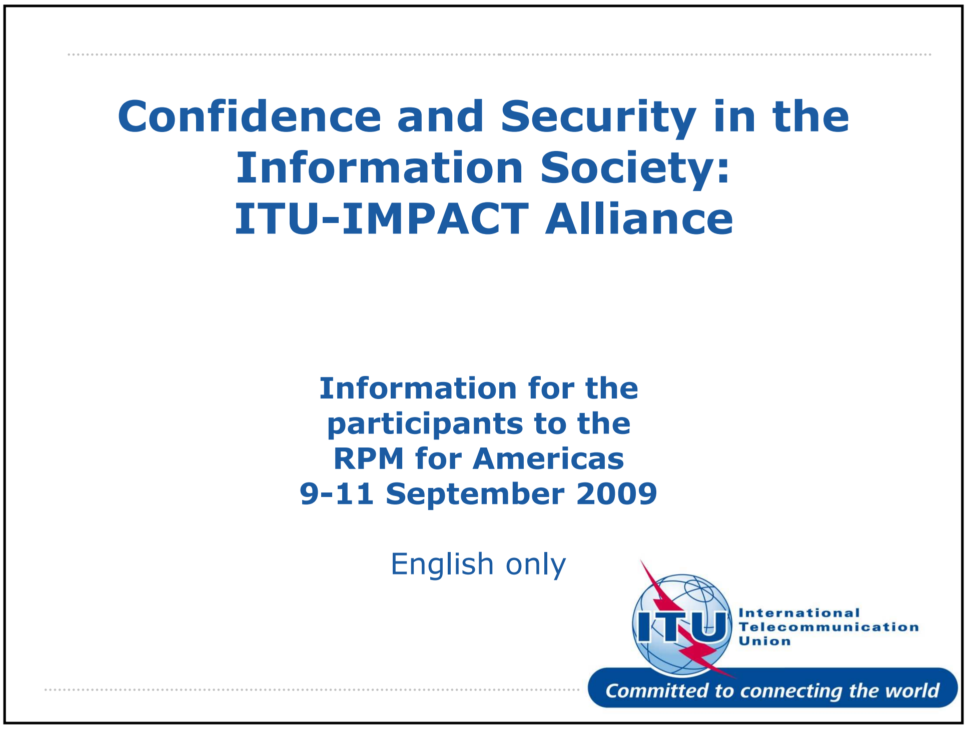
Thank you and looking forward for our future fruitful collaboration and cooperation.

Yours sincerely,

____

Date

____



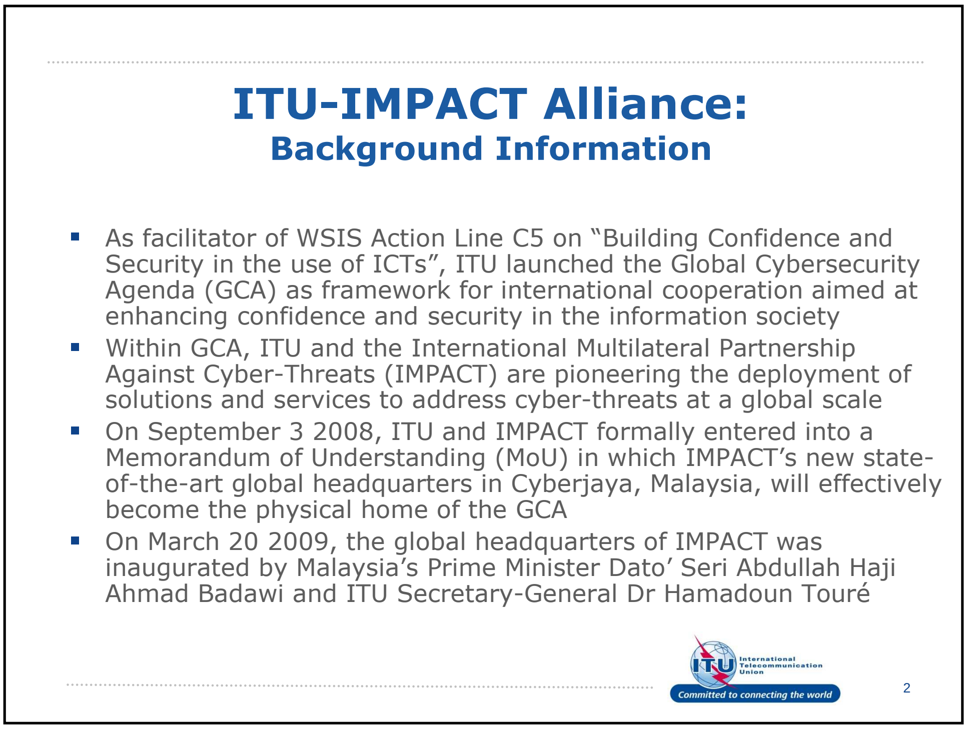
Confidence and Security in the Information Society: ITU-IMPACT Alliance

Information for the participants to the RPM for Americas 9-11 September 2009

English only

International Telecommunication Union

Committed to connecting the world



ITU-IMPACT Alliance:

Background Information

- As facilitator of WSIS Action Line C5 on “Building Confidence and Security in the use of ICTs”, ITU launched the Global Cybersecurity Agenda (GCA) as framework for international cooperation aimed at enhancing confidence and security in the information society
- Within GCA, ITU and the International Multilateral Partnership Against Cyber-Threats (IMPACT) are pioneering the deployment of solutions and services to address cyber-threats at a global scale
- On September 3 2008, ITU and IMPACT formally entered into a Memorandum of Understanding (MoU) in which IMPACT’s new state-of-the-art global headquarters in Cyberjaya, Malaysia, will effectively become the physical home of the GCA
- On March 20 2009, the global headquarters of IMPACT was inaugurated by Malaysia’s Prime Minister Dato’ Seri Abdullah Haji Ahmad Badawi and ITU Secretary-General Dr Hamadoun Touré

International Telecommunication Union

Committed to connecting the world

2

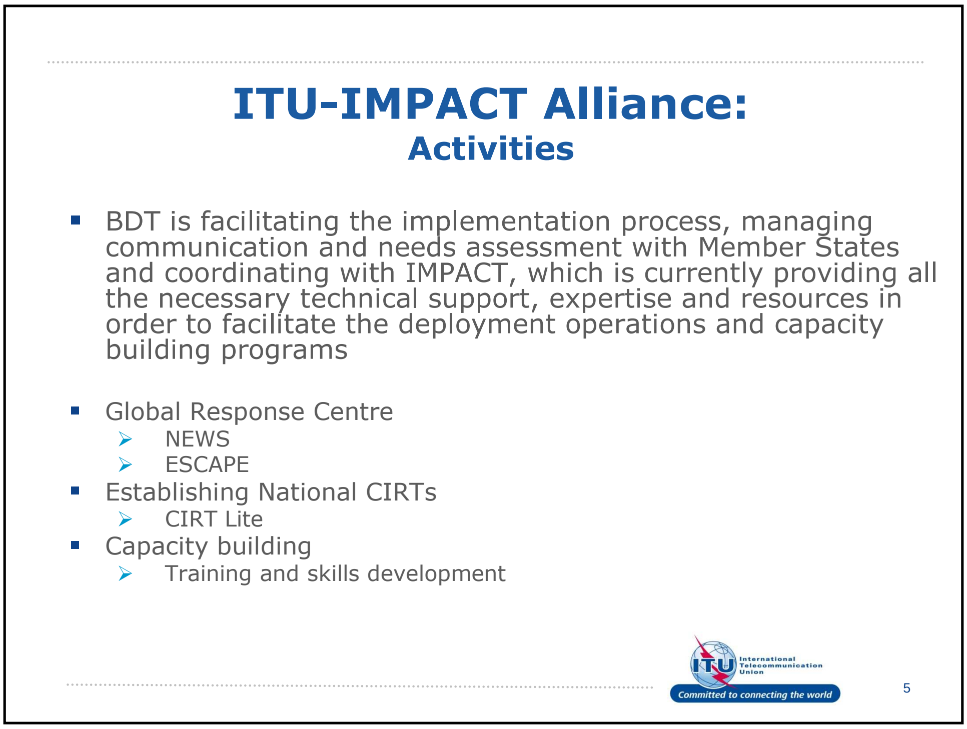
ITU-IMPACT Alliance:
Partners

- Support of key intergovernmental organizations
  - United Nations
  - International Police Organization INTERPOL
- Industry and academia
  - Symantec Corporation, Kaspersky Lab, F-Secure Corporation, Trend Micro Inc., Microsoft Corporation, Cisco Systems Inc. and Dell Inc.
- Leading cybersecurity training institutions
  - The SANS^{TM} Institute
  - The International Council of E-Commerce Consultants (EC-Council)
  - The Honeynet Project
  - (ISC)^2 Inc.

ITU-IMPACT Alliance:
Goals

In accordance with the signed MoU, the five pillars of the GCA were mapped with the tracks identified by IMPACT

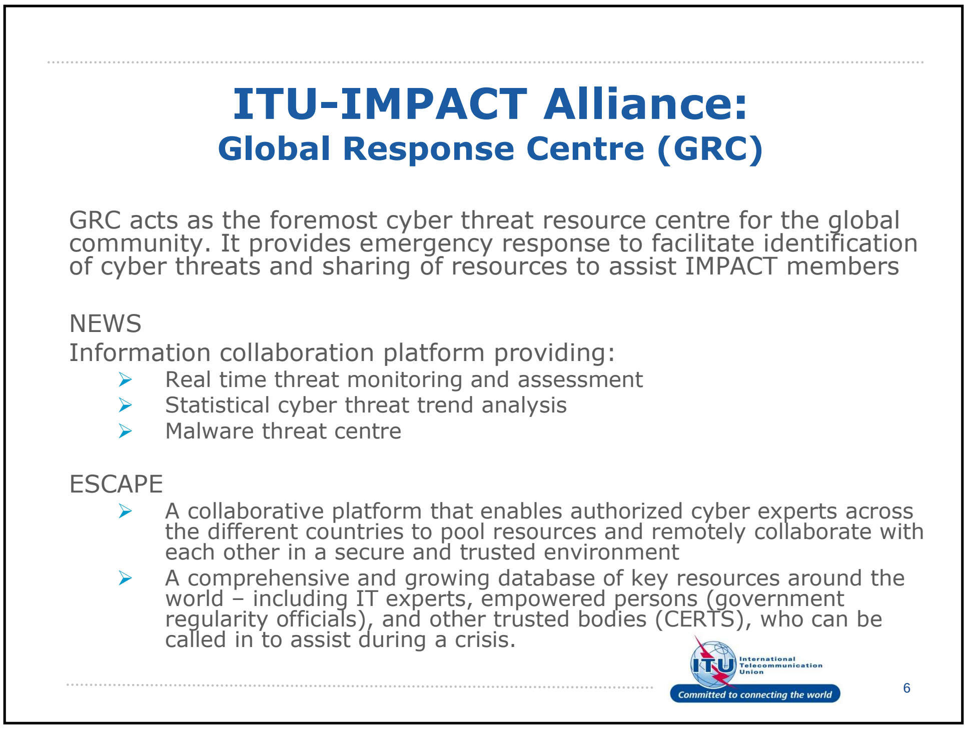
- **Legal Measures** - Elaborate strategies for the development of a model cybercrime legislation that is globally applicable and interoperable with existing national and regional legislative measures;
- **Technical and Procedural Measures** - Develop strategies for the creation of a global framework for watch, warning and incident response to ensure cross-border coordination between new and existing initiatives;
- **Organizational Structures** - Elaborate global strategies for the creation of appropriate national and regional organizational structures and policies on cybercrime;
- **Capacity Building** - Develop a global strategy to facilitate human and institutional capacity building to enhance knowledge and know-how across sectors and in all the above-mentioned areas;
- **International Cooperation** - Propose a framework for a global multi-stakeholder strategy for international cooperation, dialogue and coordination in all the above-mentioned areas



ITU-IMPACT Alliance:
Activities

- BDT is facilitating the implementation process, managing communication and needs assessment with Member States and coordinating with IMPACT, which is currently providing all the necessary technical support, expertise and resources in order to facilitate the deployment operations and capacity building programs

- Global Response Centre
  - NEWS
  - ESCAPE
- Establishing National CIRTs
  - CIRT Lite
- Capacity building
  - Training and skills development



ITU-IMPACT Alliance:
Global Response Centre (GRC)

GRC acts as the foremost cyber threat resource centre for the global community. It provides emergency response to facilitate identification of cyber threats and sharing of resources to assist IMPACT members

NEWS
Information collaboration platform providing:
- Real time threat monitoring and assessment
- Statistical cyber threat trend analysis
- Malware threat centre

ESCAPE
- A collaborative platform that enables authorized cyber experts across the different countries to pool resources and remotely collaborate with each other in a secure and trusted environment
- A comprehensive and growing database of key resources around the world – including IT experts, empowered persons (government regularity officials), and other trusted bodies (CERTS), who can be called in to assist during a crisis.

ITU-IMPACT Alliance:
Establishing National CIRTs

ITU and IMPACT have elaborated a strategy for the establishment of CIRT (Computer Incident Response Team).

CIRT Lite Project is an initiative to set up National CIRTs, providing:

- Incident Management
- Advisories
- Mailing List

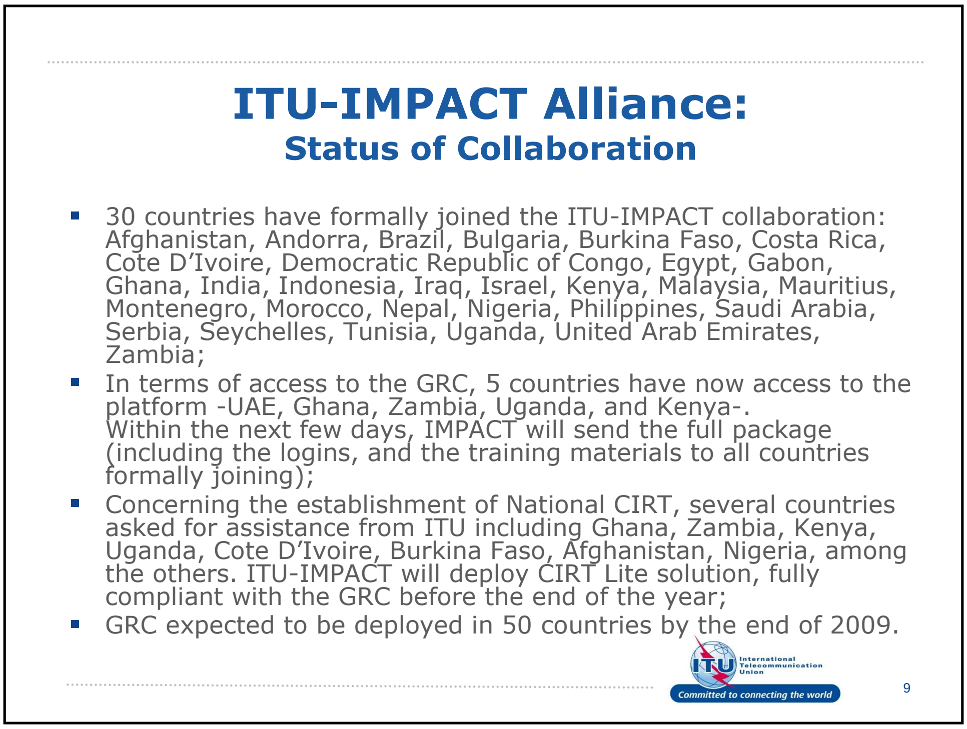
plus:

- IMPACT ESCAPE and NEWS Integration
- IMPACT Local Honeypot Deployment

ITU will support countries in the implementation of the National CIRT through the establishment of the overarching policy framework to support this technical solution and related watch, warning and incident response capabilities as part of a national strategy.

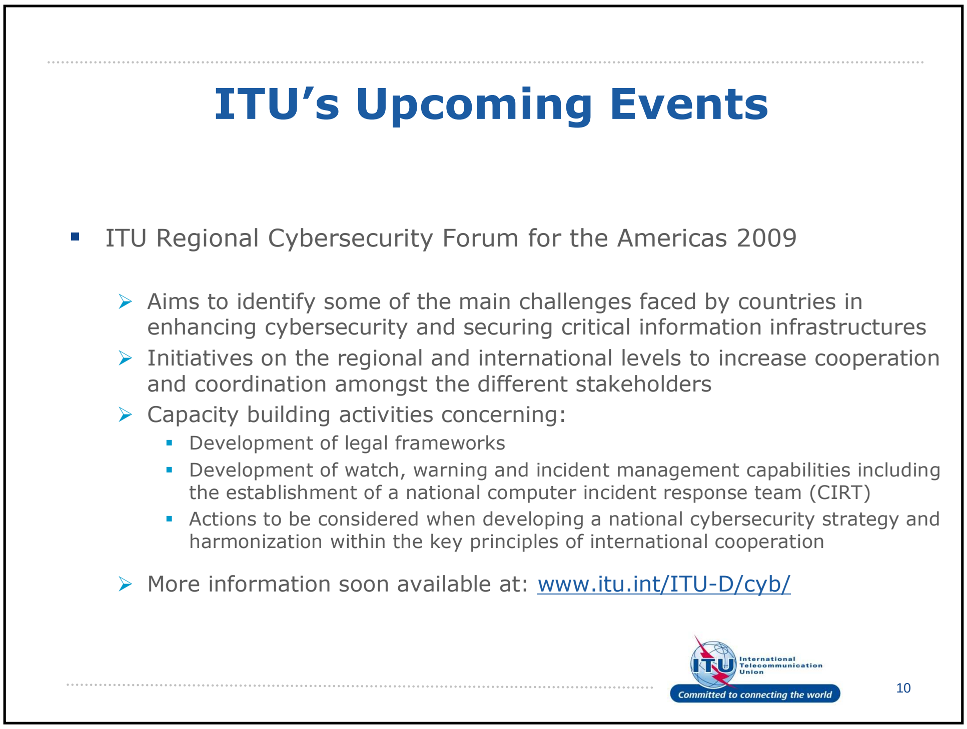
ITU-IMPACT Alliance:
Capacity Building

- ITU/BDT is coordinating with IMPACT to roll out the tools available through projects, training programs and specific applications to be integrated in the GRC
- Training and services that will be offered include:
  - SANS Scholarships for developing countries;
  - EC-Council Scholarships;
  - Other possible providers of scholarships in the future in addition to IMPACT run training courses that are currently being developed.
- CIRT staff training
  - Staffs that have been identified will be provided with the necessary basic skill training in order for them to be able to perform the basic incident response and handling functions;
  - These training will be sponsored for the countries and for a specific number of staffs that will be determined accordingly;
  - Training of the staffs will be done for both management and technical to ensure that relevant skill sets are adequately present in the team.



ITU-IMPACT Alliance:
Status of Collaboration

- 30 countries have formally joined the ITU-IMPACT collaboration: Afghanistan, Andorra, Brazil, Bulgaria, Burkina Faso, Costa Rica, Cote D'Ivoire, Democratic Republic of Congo, Egypt, Gabon, Ghana, India, Indonesia, Iraq, Israel, Kenya, Malaysia, Mauritius, Montenegro, Morocco, Nepal, Nigeria, Philippines, Saudi Arabia, Serbia, Seychelles, Tunisia, Uganda, United Arab Emirates, Zambia;
- In terms of access to the GRC, 5 countries have now access to the platform -UAE, Ghana, Zambia, Uganda, and Kenya-.
  Within the next few days, IMPACT will send the full package (including the logins, and the training materials to all countries formally joining);
- Concerning the establishment of National CIRT, several countries asked for assistance from ITU including Ghana, Zambia, Kenya, Uganda, Cote D'Ivoire, Burkina Faso, Afghanistan, Nigeria, among the others. ITU-IMPACT will deploy CIRT Lite solution, fully compliant with the GRC before the end of the year;
- GRC expected to be deployed in 50 countries by the end of 2009.



ITU's Upcoming Events

- ITU Regional Cybersecurity Forum for the Americas 2009
  - Aims to identify some of the main challenges faced by countries in enhancing cybersecurity and securing critical information infrastructures
  - Initiatives on the regional and international levels to increase cooperation and coordination amongst the different stakeholders
  - Capacity building activities concerning:
    - Development of legal frameworks
    - Development of watch, warning and incident management capabilities including the establishment of a national computer incident response team (CIRT)
    - Actions to be considered when developing a national cybersecurity strategy and harmonization within the key principles of international cooperation
  - More information soon available at: www.itu.int/ITU-D/cyb/

Links to More Information

- ITU-IMPACT Resources
  - www.itu.int/ITU-D/cyb/cybersecurity/impact.html
- An Overview of ITU Activities in Cybersecurity
  - www.itu.int/cybersecurity/
- ITU Global Cybersecurity Agenda
  - www.itu.int/cybersecurity/gca/
- ITU-D ICT Applications and Cybersecurity Division
  - www.itu.int/ITU-D/cyb/
- ITU Cybercrime Legislation Resources
  - www.itu.int/ITU-D/cyb/cybersecurity/legislation.html
- Regional Cybersecurity Forums and Conferences
  - www.itu.int/ITU-D/cyb/events/
- ITU Child Online Protection (COP)
  - www.itu.int/cop/

Thank You!

For more information on
ITU’s Cybersecurity Activities
visit the website at:
www.itu.int/cybersecurity/

or contact cybmail@itu.int