GLOBAL CYBERSECURITY AGENDA

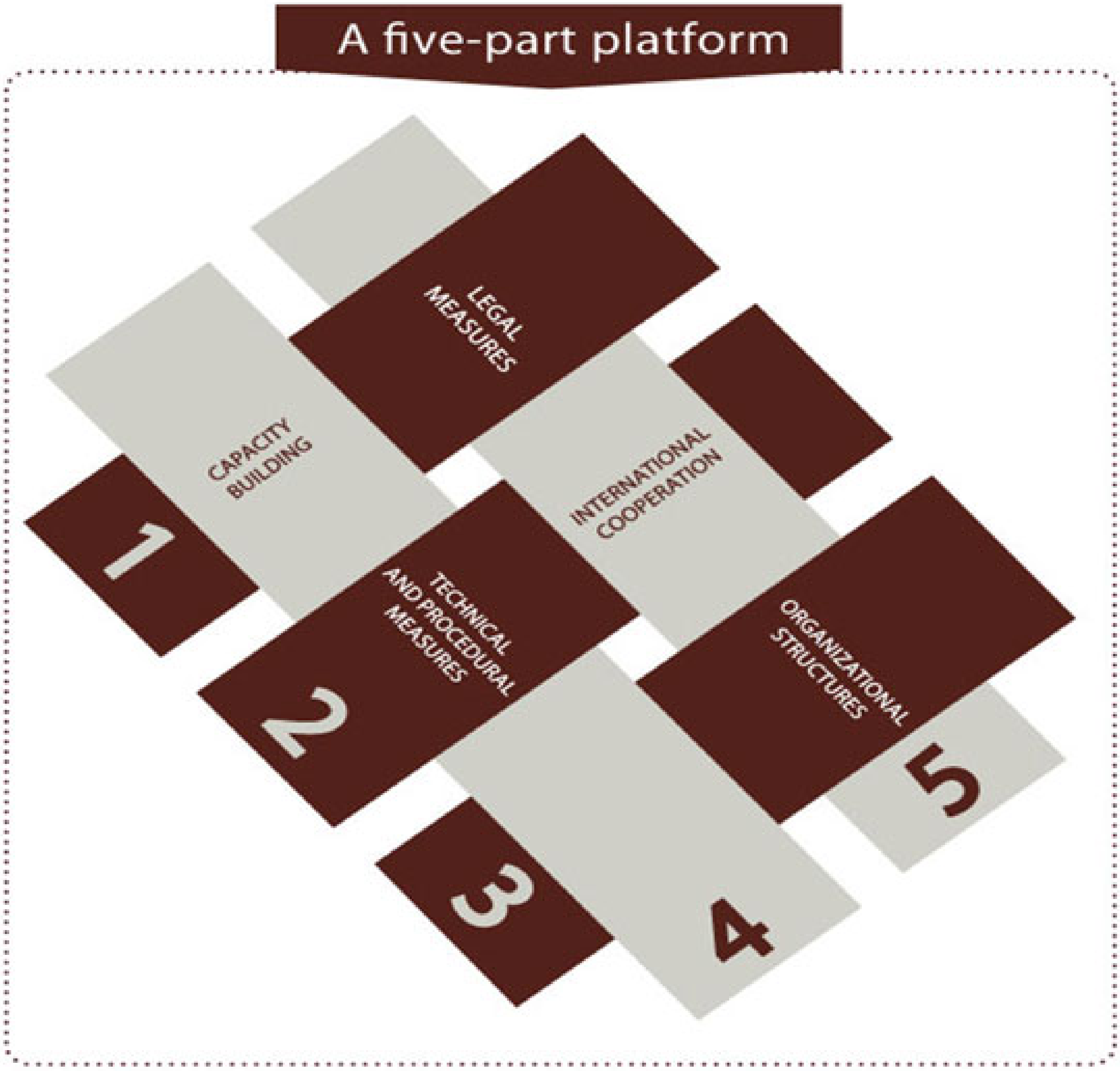
ITU (International Telecommunication Union) recognizes that information and technology security are critical priorities for the international community. Cybersecurity is in everyone's best interest and this can only be achieved through collaborative efforts. Cyber threat issues are global and therefore their solutions must be global too.

It is vital that all countries arrive at a common understanding regarding cybersecurity, namely by providing protection against unauthorized access, manipulation and destruction of critical resources. ITU believes that in developing a solution one must identify all existing national and regional initiatives, in order to foster collaboration with its multiple stakeholders and avoid duplication of efforts. With its 191 Member States and more than 700 Sector Members, ITU is uniquely placed to propose a framework for international cooperation in cybersecurity and assist in tackling cybercrime.

The World Summit on the Information Society (WSIS), which met in Geneva in 2003 and in Tunis in 2005, called upon ITU to act as the sole Facilitator of Action Line C5, "Building confidence and security in the use of ICTs". On 17 May 2007, ITU Secretary-General, Dr. Hamadoun I. Touré, launched the Global Cybersecurity Agenda (GCA) which is a framework for international cooperation aimed at enhancing confidence and security in the information society. A multi-stakeholder High Level Experts Group (HLEG) comprising of more than one hundred experts from Governments, Industry, International organizations, NGOs and academic institutions was established to further develop main goals, analyse current developments in all areas of cybersecurity and formulate proposals on possible long-term strategies and emerging trends in cybersecurity. In 2008, the HLEG put together the Global Strategic Report which provided recommendations on key steps forward for all five pillars of the GCA.

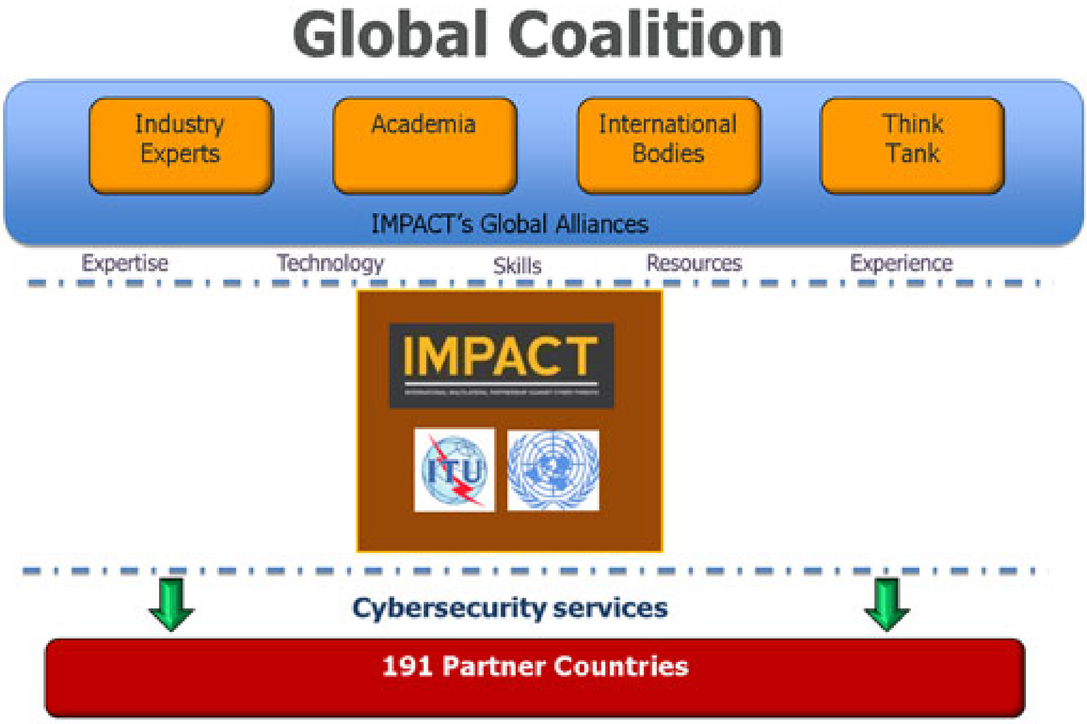
The GCA is a multi-stakeholder approach designed to promote collaborative work across the sectors of ITU namely, the Radiocommunication Sector (ITU-R), the Standardization Sector (ITU-T) and the Telecommunication Development Sector (ITU-D). It has fostered initiatives such as Child Online Protection, launched the Cybersecurity Gateway and through its partnership with IMPACT and with the support of leading global players is currently deploying cybersecurity solutions to countries around the world.
The GCA is built upon five strategic pillars, also known as work areas, and made up of seven main strategic goals.
The Five Pillars/Work Areas:

1. Legal Measures
2. Technical and Procedural Measures
3. Organizational Structures
4. Capacity Building
5. International Cooperation


A five-part platform
LEGAL MEASURES
CAPACITY BUILDING
INTERNATIONAL COOPERATION
TECHNICAL AND PROCEDURAL MEASURES
ORGANIZATIONAL STRUCTURES
1
2
3
4
5

Legal Measures

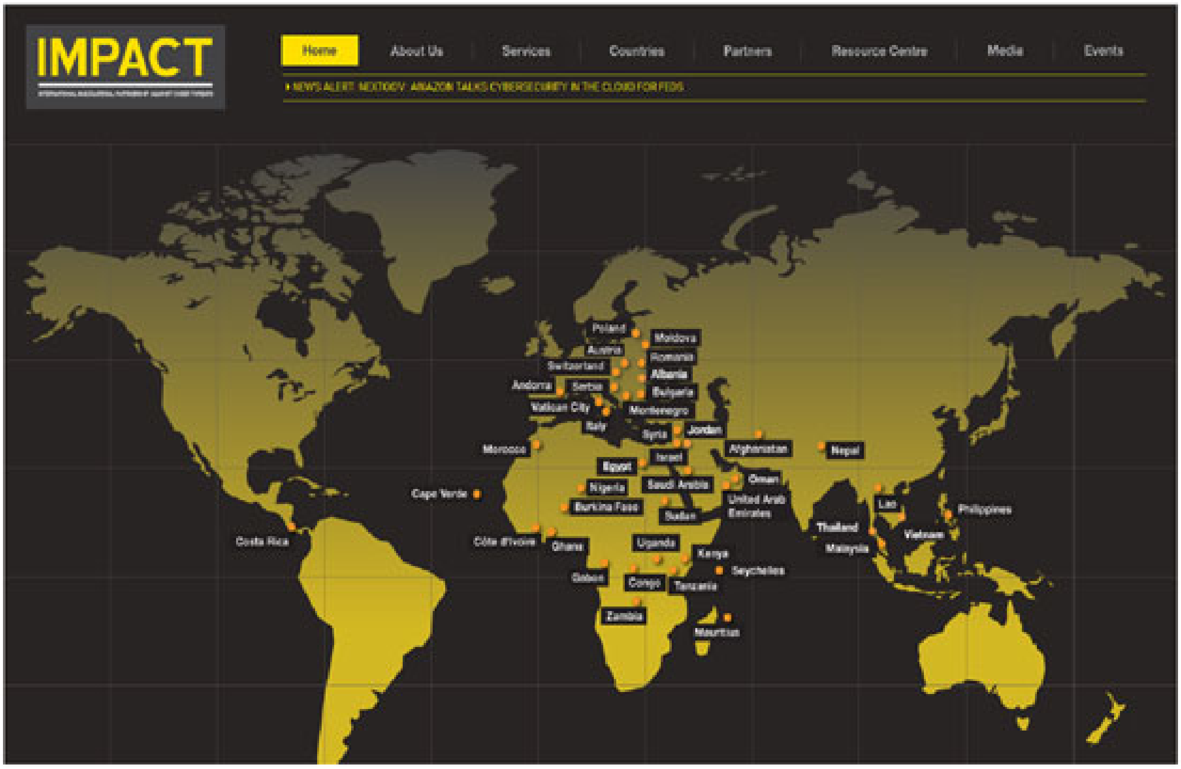
To better understand the legal aspects of cybersecurity ITU has devised cybercrime legislation resources. With these resources, ITU is working to assist countries in moving towards harmonizing legal frameworks. This activity also addresses the ITU-D Study Group Q22/1 approach for organizing national cybersecurity efforts, highlighting that establishing the appropriate legal infrastructures is an integral component of a national cybersecurity strategy.
The ITU cybercrime legislation resources currently consist of two main deliverables, the ITU publication titled ITU Toolkit for Cybercrime Legislation and Understanding Cybercrime: A Guide for Developing Countries.
ITU- IMPACT Collaboration
As the world’s first non-profit comprehensive global public-private partnership against cyber threats, the International Multilateral Partnership Against Cyber Threats (IMPACT) is well positioned to assist partner countries, especially developing nations who are broadening their Internet capabilities.



On 3 September 2008, IMPACT and the ITU formally entered into a Memorandum of Understanding (MoU) in which IMPACT's state-of-the-art Global HQ in Cyberjaya, Malaysia, effectively became the physical and operational home of the GCA. Under this landmark collaboration, IMPACT provides the ITU's 191 Member States with the expertise, facilities and resources to effectively address the world's most serious cyber threats.
The partnership provides:

- Real-time analysis, aggregation and dissemination of global cyber-threat information;
- Network Early Warning System (NEWS) and emergency response to global cyber-threats; and
- Training and skills development on the technical, legal and policy aspects of cybersecurity.

Current Deployment Status



IMPACT

Home | About Us | Services | Countries | Partners | Resource Centre | Media | Events

NEWS ALERT: NEXTGOV: AMAZON TALKS CYBERSECURITY IN THE CLOUD FOR FEDS

Below is an alphabetical list of countries which have already joined ITU-IMPACT collaboration:

IMPACT's Key Partners

Industry

International Organisations

Academia

+ 200 more

Child Online Protection (COP)

Under the GCA umbrella, the ITU launched the Child Online Protection (COP) initiative in November 2008. The COP initiative has been established as an international collaborative network for action to promote the online protection of children and young people worldwide by providing guidance on safe online behaviour in conjunction with other UN agencies and partners. It addresses the legal, technical, organizational and procedural issues as well as capacity building and international cooperation.

Since its launch, COP has attracted the support and recognition of leaders and experts from around the world. More recently, the President of Costa Rica Mme. Laura Chinchilla accepted the invitation to be the Patron of this initiative.
The key objectives of the initiative are to:

1. Identify the key risks and vulnerabilities to children and young people in cyberspace;
2. Create awareness of the risks and issues through multiple channels;
3. Develop practical tools to help governments, organizations and educators minimize risk;
4. Share knowledge and experience while facilitating international strategic partnerships to define and implement concrete initiatives.

Cybersecurity Gateway

The purpose of the ITU Cybersecurity Gateway is to provide an easy-to-use information resource on national, regional and international cybersecurity-related initiatives worldwide.
In today’s interconnected world of networks, threats can originate anywhere, and thus our collective cybersecurity depends on the security practices of every connected country, entity, business, and citizen. National and international cooperation is needed among those who seek to promote, develop and implement initiatives for a global culture of cybersecurity. Through the Cybersecurity Gateway, ITU aims to enable information access, dissemination and online collaboration among stakeholders working in cybersecurity and related areas. The Gateway provides a platform to share information between partners in civil society, the private sector, governments and international organisations working on enhancing cybersecurity. The ITU invites all interested parties to explore the vast resources and links available through the Cybersecurity Gateway and join in partnership with the ITU and others to build confidence and security in the use of ICTs. The Cybersecurity Gateway has been recently updated with a newer version.

Conclusion

It is undeniable that ICTs form an integral part of society today and that they will continue to do so in the future, with the Internet connecting ever more parts of the world. ICTs are constantly evolving, progressing and improving many aspects of our lives. This also rings true for cyber threats as they are intrinsically linked to ICT evolution. The ITU is very serious towards its responsibility for WSIS Action Line C5, “Building confidence and security in the use of ICTs”, and is working hard to address the emerging challenges of the Information Society. The Global Cybersecurity Agenda as an international framework has helped ITU take a leadership role in both cybersecurity issues and in WSIS implementation. It has helped build awareness of ITU’s activities among experts within the field and won their commitment and ownership of the strategies developed by the HLEG.
The GCA continues onwards, forming partnerships and enabling ITU Sectors to implement these strategies through concrete activities. Much has been achieved but cybersecurity is a constantly evolving challenge,

which needs to be continually addressed due to the ever changing nature of ICTs. ITU will persistently work to build confidence and trust to ensure a safe and secure cyber environment for all.

For more information log on to: www.itu.int/cybersecurity
Contact: cybersecurity@itu.int