Global Cybersecurity Agenda (GCA)

Despite ITU's already active involvement in cybersecurity, there was a feeling that more could be done. Largely because of ITU's long and successful history of forging consensus on the way the world manages globally shared ICT resources - such as satellite orbits and radiofrequency spectrum, ITU was given the task to build an international framework of cybersecurity principles and best practice that countries around the world could follow, maximizing and coordinating efforts to stamp out cybercrime.

Launched officially by Dr Hamadoun Touré, ITU Secretary General on 17 May 2007, the Global Cybersecurity Agenda (GCA) was ITU's answer to the urgent request stemming from the 2005 World Summit on the Information Society (WSIS) for a global consensus on cybersecurity. The GCA has mobilized a multi-stakeholder team of interested stakeholders (including governments, private sector, civil society, and international organizations) in the High-Level Experts Group (HLEG), which has advised the ITU Secretary-General on long-term strategies to promote cybersecurity.

What makes the GCA Unique?

The GCA's role is to link existing initiatives and provide an overarching framework for consensus. This allows each stakeholder Group to focus on its own mandate, while ensuring cooperation with other stakeholders. The GCA already has Interpol - the global organization for international law enforcement, with 186 member states - sharing ideas with UNODC, the United Nations Office on Drugs and Crime. Both these organizations are putting heads together with the likes of APECTEL (Asia Pacific Economic Telecommunications and Information Working Group) and UNITAR (United Nations Institute for Training and Research). By working together in this manner, our chances of success on an international level are increased significantly. And by involving global experts in the process from the beginning, we help to ensure that the solutions decided upon get implemented properly. Everyone recognizes that working together is the only way forward. A piecemeal approach to cybercrime is like the proverbial chain - it is only as strong as its weakest link.

Like its logo, the GCA is designed around five major pillars:

1. **Legal Measures:** development of model cybercrime legislation that is globally applicable and interoperable with existing policies;
2. **Technical and Procedural Measures:** global strategies for addressing vulnerabilities in software products, including accreditation schemes, protocols and standards;
3. **Organizational Structures:** a generic framework and optimal response strategies for the prevention, detection, response to and crisis management of cyberattacks, including the protection of countries' critical information infrastructure systems;
4. **Capacity Building:** elaborating strategies for concrete capacity-building mechanisms to raise awareness, transfer know-how and boost cybersecurity on the national policy agenda;
5. **International Cooperation:** multi-stakeholder strategy for international cooperation, dialogue and coordination in dealing with cyberthreats.

From recommendation to reality

Since the launch of the GCA, the HLEG has been busy creating recommendations on actions to be undertaken in the five work areas of the GCA. Its outputs are represented in a strategic report on each of the five work areas and the Report of the Chairman of the HLEG to the ITU Secretary-General, which contains all proposals tabled by HLEG members. The Chairman's Report further summarizes the work of the HLEG, the views expressed by HLEG members and other information about the work carried out by HLEG, since its inception. Some of the proposals were taken into consideration by ITU Secretary General. Those proposals that were considered have been reviewed by all three ITU Sectors, linked to the relevant ITU mandate and are being taken into account in work programmes of the Sectors.

Please see the Report of the Chairman of HLEG to ITU Secretary-General available at: http://www.itu.int/osg/csd/cybersecurity/gca/docs/Report_of_the_Chairman_of_HLEG_to_ITU_SG_03_sept_08.pdf

Outcomes and achievements of the GCA and HLEG

During the year since its launch, the GCA has achieved some notable successes, including endorsement by the WSIS stakeholder community during the 2008 WSIS Action Line C5 Facilitation Meeting as a credible multi-stakeholder global framework for international cooperation in addressing the global challenges in cybersecurity. The Internet Governance Forum (IGF) has also endorsed the GCA as a model for international cooperation in cybersecurity. The GCA initiative has helped ITU assume a leadership role, in both cybersecurity issues and in WSIS implementation.

Through the GCA, ITU's reputation as a forum for international cooperation has been further reinforced. The GCA 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. With its diverse public-private sector membership (including 191 Member States and more than 700 Sector Members and Associates), ITU is uniquely placed to serve as a global forum for the development of a framework for international cooperation in cybersecurity. The GCA has facilitated the establishment of multi-stakeholder partnerships with new, external partners to promote cybersecurity.

The GCA has helped mobilize and has benefited from the expertise of more than one hundred high-level experts from a broad range of different sectors and geographical regions. The GCA has helped forge a common understanding of cybersecurity threats among countries at all stages of economic development. The HLEG formulated a set of proposals in all five work areas of GCA, five strategic reports and a Chairman's report, which includes all the work carried out by HLEG in addressing a wide range of challenges and issues related to the fight against cybercrime and the promotion of global cybersecurity.

In affirmation of the international recognition given to the GCA, Dr. Óscar Arias Sánchez, President of the Republic of Costa Rica and Nobel Peace Laureate, as well as Mr. Blaise Compaoré, President of Burkina Faso, kindly accepted to be the Patrons of the GCA.

Many Member States, through their Ministers and other senior level officials, have endorsed the GCA as a framework for international cooperation in cybersecurity. Furthermore, regional institutions, such as the African Union, have offered to collaborate under the GCA umbrella.

The GCA has also strengthened ITU's role as a key player in cybersecurity and raised its profile and visibility worldwide. The ITU and GCA have been widely referenced in mainstream media as a major forum for international cooperation in cybersecurity.

The momentum generated by the GCA and the broad nature of this ITU initiative have resulted in interest from other stakeholders and opportunities for collaboration and cooperation. Specific initiatives already undertaken under GCA umbrella include**:**

IMPACT & GCA

The Government of Malaysia offered to make available the infrastructure of the International Multilateral Partnership Against Cyber-Terrorism (IMPACT) as the home of the GCA. IMPACT is backed by a US$ 13 million infrastructure and has agreed to make its state-of-the-art global headquarters in Cyberjaya, Kuala Lumpur, available as one of the physical homes of ITU's Global Cybersecurity Agenda. IMPACT has agreed to make available its infrastructure and services to meet the GCA goals in its five work areas.

The collaboration between ITU and IMPACT is based on a Memorandum of Understanding (MoU) signed in Bangkok during ITU TELECOM ASIA 2008 by ITU Secretary-General, Dr Hamadoun Touré, and the Chairman of the IMPACT Management Board, Mr Mohammad Noor Amin. It seeks to build synergies to provide:

- Real-time analysis, aggregation and dissemination of global cyber-threat information;
- Early warning system and emergency response to global cyber-threats; and
- Training and skills development on the technical, legal and policy aspects of cybersecurity.

Under the terms of this MoU, the GCA is to be housed at the IMPACT Centre, while ITU will maintain a ‘virtual showcase’ in Geneva of the early warning system, crisis management and real-time analysis of global cyber-threats. IMPACT initiatives, such as the Global Response Centre, as well as training and skills development, security assurance, research, and international cooperation, are being conducted under the auspices of the GCA. This agreement is in line with the decision of the WSIS to build security and confidence in the use of ICTs.

Microsoft & GCA

In accordance with Resolution 130 (Rev. Antalya 2006) regarding the Cybersecurity Gateway, ITU proposed a structure for collecting and sharing information on cybersecurity initiatives worldwide to the Third WSIS Action Line C5 Facilitation Meeting on 22-23 May 2008. ITU signed a Memorandum of Understanding with Microsoft during the *Connect Africa Summit* in Kigali, Rwanda, in October 2007 to enhance the Cybersecurity Gateway using technology developed for the ITU Global View project. Agreements have been reached for cooperation in a number of areas, including assistance from Microsoft in enhancing the cybersecurity gateway and capacity-building activities with the BDT.

Child Online Protection Initiative (COP) & GCA

The Child Online Protection Program (COP) is an international collaborative network based on a multi-stakeholder and multi-sectoral partnership for joint action to promote the online protection of children worldwide, through education and awareness-raising on e-safety, facilitating the development and use of appropriate technologies, including a framework for cooperation among relevant stakeholders in the protection of children online. The Child Online Protection Initiative will be implemented as a project with well-defined objectives through cooperation between BDT and eWorldwide Group, with the participation of a wide range of stakeholders.

The COP will draw together an effective package of policies and practices, education and training, and infrastructure and technology, underpinned by an awareness and communications strategy that addresses the needs of all the stakeholders that have a role to play within this environment. Activities on e-safety issues by a wide range of organizations will be studied and solicited, in order to develop a common framework for the protection of children online. Critical awareness, effective security practices, digital literacy and good online citizenship will provide focused activities for children and continuing professional development for practitioners to enhance their knowledge and understanding in this area. A clear standards-based approach will help ensure that infrastructures designed today are able to offer secure ICTs to avoid any possibility of misuse.

More information can be found at: http://www.itu.int/cybersecurity/gca/ or by contacting Corporate Strategy Division (CSD/SPM) at gca@itu.int