GCA STRATEGY

Five pillars of the ITU Global Cybersecurity Agenda

The ITU Global Cybersecurity Agenda is built upon five (5) strategic pillars:

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

The legal framework, technical measures and organizational structures need to be undertaken at the national and regional levels but also harmonized at the international level. The last two pillars, capacity building and international cooperation, cross-cut in all areas (see figure on last page). In order to carry out its Agenda, ITU will fully engage its Member States and all the world's players in its activities. It will collaborate closely with its partners to identify current challenges, consider emerging and future threats, and propose global strategies to meet the goals of the Agenda.

The Global Cybersecurity Agenda will facilitate the implementation of activities aimed at meeting ITU's Strategic Goals in this domain by developing and proposing forward looking global strategies using a wide range of expertise and taking account of existing initiatives.

Setting achievable goals

The Global Cybersecurity Agenda is made up of seven main strategic goals:

1 Elaboration of strategies for the development of a model cybercrime legislation that is globally applicable and interoperable with existing national and regional legislative measures.
2 Elaboration of strategies for the creation of appropriate national and regional organizational structures and policies on cybercrime.
3 Development of a strategy for the establishment of globally accepted minimum security criteria and accreditation schemes for software applications and systems.

4 Development of strategies for the creation of a global framework for watch, warning and incident response to ensure crossborder coordination between new and existing initiatives.

5 Development of strategies for the creation and endorsement of a generic and universal digital identity system and the necessary organizational structures to ensure the recognition of digital credentials for individuals across geographical boundaries.

6 Development of 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.

7 Proposals on a framework for a global multi-stakeholder strategy for international cooperation, dialogue and coordination in all the above-mentioned areas.

High-Level Experts Group on Cybersecurity (HLEG)

In order to assist ITU's Secretary-General in developing strategic proposals to Member States, he will seek the advice of the High-Level Experts Group on strategies in all five work areas or pillars.

The HLEG will comprise a group of high-level experts from governments, industry, relevant regional/international organizations, research institutes, academic institutions and individual experts from every part of the world appointed by the ITU Secretary-General.
The work of HLEG will be funded primarily through voluntary contributions (cash and inkind) from its members and other donors.

Main responsibilities of HLEG to the ITU Secretary-General

- To further develop the Global Cybersecurity Agenda, by proposing refinements to its main goals.
- To analyse current developments in cybersecurity, including both threats and state-of-the-art solutions, anticipate emerging and future challenges, identify strategic options, and formulate proposals to the ITU Secretary-General.
- To meet the goals of the Global Cybersecurity Agenda.
- To provide guidance on possible long-term strategies and emerging trends in cybersecurity.

Composition of HLEG

Members of the HLEG will be nominated by the ITU Secretary-General, with due consideration to both geographical diversity and expertise in the five pillars or work areas of the Global Cybersecurity Agenda. General features and characteristics of HLEG include:

- A global multi-stakeholder think-tank made up of high level experts from governments, industry, international organizations, research and academic institutions and individual experts.
- To ensure balance in the membership of HLEG, its members will be nominated as follows:

a) Member States – government representatives of countries from the five world regions

b) Industry – manufacturers, operators, service providers, software developers, security and other information technology firms

c) Regional/International organizations

d) Research and academic institutions

e) Individual experts