International Telecommunication Union

ITU Global Cybersecurity Agenda (GCA)

Framework for International Cooperation in Cybersecurity

International
Telecommunication
Union

Table of contents

a Background

The crucial role that confidence and security play as one of the main pillars in building an inclusive, secure and global information society was one of the main conclusions of the World Summit on the Information Society (WSIS).

The global nature of the legal, technical and organizational challenges related to cybersecurity can only be properly addressed through a strategy that takes account of the role to be played by all relevant stakeholders, existing initiatives in a framework of international cooperation.

Attempts to address these challenges at the national and regional levels are not sufficient due to the fact that the information society has no definite geographical borders.

ITU has been entrusted by the WSIS community of stakeholders to facilitate the implementation of WSIS Action Line C5 (Building confidence and security in the use of ICTs). With its 191 Member States and more than 700 Sector Members, ITU is uniquely placed to propose a framework for international cooperation in cybersecurity. Its membership includes the least developed, developing and emerging economies as well as developed countries. ITU therefore provides a forum where these diverse views of what cybersecurity and cybercrime mean to various countries can be discussed, with the goal of arriving at a common understanding amongst countries on how these challenges can be addressed.

The Global Cybersecurity Agenda (GCA) is an ITU framework for international cooperation aimed at proposing solutions to enhance confidence and security in the information society. It will build on existing national and regional initiatives to avoid duplication of work and encourage collaboration with all relevant partners.

The changing nature of cyberthreats and their constant evolution

There have been significant changes in the level of sophistication of cyberthreats since 1986 when the first known case of a computer virus aimed at advertising a Computer Store in Lahore, Pakistan, was reported. Just a few years ago, the development and dissemination of malware (viruses, worms, and Trojans) was essentially to demonstrate the technical skills of information technology (IT) professionals. Today, we are dealing with a new form of organized cybercrime aimed at financial gains, with an expansion of the types of threats to various platforms and to various countries. Spam has evolved to become a vehicle for delivering more dangerous payloads, such as the dissemination of viruses, worms and Trojans that are today a means for online financial fraud, identity or trade-secret theft as well as various other forms of cyberthreats.

When threats to critical infrastructures in the financial, health, energy, transportation, telecommunication, defence and other sectors are taken into account, it is obvious that the situation is likely to get worse.

One of the emerging and rather dangerous trends is the shift in strategy by hackers from the central command-and-control model for controlling botnets to a peer-to-peer model with a distributed command structure capable of spreading to computers located in different countries. This makes it very difficult to pinpoint one geographical location as the origin of these attacks, and consequently makes it difficult to identify them and shut them down. This shift strategy is not just aimed at delivering spam with more dangerous payloads but can also be used to disseminate inappropriate content, such as child pornography, without the knowledge of the hijacked computer owners that they are hosting and disseminating such content.

Lower entry barrier and ease of acquiring cybercrime toolkits

Toolkits and applications for phishing, spam, malware, scareware and snoopware can be relatively easily acquired today from underground sites or even purchased legally, thereby lowering the financial and intellectual entry barriers to acquire tools aimed at the unauthorized access, manipulation and destruction of information and information systems.

Snoopware is going mobile, threatening user privacy through the possibility of voice/data call monitoring with potentially devastating consequences, especially for the growing number of corporate users who rely on their smartphones for confidential discussions and data exchanges with their corporate IT systems. With the phenomenal growth in mobile (including smartphones), especially in developing countries, together with the process of convergence which brings down barriers between what used to be different networks, one can see how these threats can easily spread to all countries and to all platforms.

As information technology becomes more and more part of our lives with computers becoming components in a number of household appliances, and as ubiquitous connections to the Internet become a reality, there is a high chance that cyberthreats will spread to new levels and affect us in ways not known today.

Legal aspects: Loopholes in current legal frameworks

Cybercriminals are already exploiting vulnerabilities and loopholes in national and regional legislation as they shift their operations to countries where appropriate and enforceable laws are not yet in place, and can, with almost total impunity, even launch attacks on victims in countries which do have laws in place.

When several hijacked computers and networks that have been compromised spread over many countries and are used to launch cyberattacks using a decentralized model (based on peer-to-peer arrangements), no national or regional legal framework can adequately deal with such a problem. This challenge can only be addressed globally.

Many countries have adopted or are working on legislation to combat cybercrime and other misuses of information technology. These laws are drawn up to be enforceable in well defined geographical boundaries that are either national or regional. But even if all countries had laws, a cybercriminal operating in Country A cannot be easily extradited to Country B where the crime has been committed, unless these legal frameworks are inter-operable, and this is not the case today. Efforts to address this challenge have been made by establishing bilateral agreements and various Memoranda of Understanding between countries. However, this model has its limitations because of the complexities in managing numerous bilateral agreements, especially when countries need to extend such agreements to many countries. Another limitation of this strategy is the undesirable effects of trust cascades, resulting where, say, five countries are signatories of one agreement (first agreement) and one of these countries signs another bilateral agreement with a sixth country. Does that imply that the five parties that are signatories of the first agreement agree to extend this cooperation to the sixth country?

Clearly, these attempts – even though valuable – are not the solution to the global nature of the legal challenges faced today. In fact, they can only result in shifting the problem from one country to the next, and creating mobile cybercrime-heavens for cybercriminals who cannot be bound to any territorial jurisdiction.

Technical measures: Vulnerabilities of software applications

Many of the threats we face today, such as malware (viruses, worms and Trojans), are due to a wide range of issues including vulnerabilities in software applications that are exploited in order to gain unauthorized access to information and information systems. As access to information is facilitated by the borderless nature of the information society, so is access to vulnerable software applications and systems.

As efforts are made to reduce the impact of spam as a transport mechanism for the dissemination of malware and other forms of misuse of information technology, cybercriminals are changing strategies and exploiting vulnerabilities in software applications to launch their attacks through web-based applications. While the industry is well organized for addressing vulnerabilities in security software through a number of standards, accreditation schemes and certification, not much is being done to address the shortfall of applications on which many users, businesses, companies and governments rely for the delivery of services, some of which are critical in domains such as health, finance, commerce and public administration. For developing countries that rely on ICT applications to enhance access to some basic services such as e-health, e-government and e-commerce, the threats posed by the recurring nature of exploiting software vulnerabilities in order to gain unauthorized access and control of information systems and the destruction of critical data cannot be overestimated. These could, for example, result in the modification of critical medical data, with results that could go far beyond financial losses.

There are regional and national initiatives to address the challenges related to standardizing methods of accreditation for software applications in order to reduce their vulnerabilities and make it safer for access to the information society. These efforts are focused mostly on security applications and devices. They need to be extended to normal applications. It is therefore vital to leverage the experience of the software and hardware security industry, take account of these existing initiatives and expertise and elaborate strategies within a framework of international cooperation to put in place accreditation schemes, protocols and standards. These must address the security vulnerabilities exploited today by cybercriminals to gain access and control to information systems and data.

Organizational structures: Absence of appropriate organizational structures

The absence of structures to deal with incidents (such as virus and network attacks that could result in fraud, the destruction of information, and the dissemination of inappropriate contents) is a real problem when attempting to combat cybercrime and respond to cyberattacks.

While some countries and regions have set up structures for incident response, watch and warnings, and have put in place the organizational structures for coordinating responses to incidents and applying procedures related to cybersecurity, much more still needs to be done. Usually, when a cyberattack occurs in one country, the devastating effects reach victims in other connected countries, without the necessary information-flow, collaboration and cooperation between national organizational structures for dealing with how to handle and respond to such incidents.

Another area where is it necessary to put in place organizational structures and appropriate policies and procedures is in the domain of generic identity certificates (digital certificates), which has been recognized as one of the vital strategies in combating cyberthreats (identity theft, phishing and other forms of online fraud). Strong authentication is one important component for building confidence and security in the information society. While some countries have established the organizational structures and infrastructure to provide generic identity certificates to citizens, it is necessary to facilitate the establishment of such structures in other countries and put in place a global framework to enable government-run national generic identity certificates to be recognized globally across geographical boundaries.

Efforts have been made to bring together some of these organizational structures, mostly at the national and regional levels, in order to facilitate communication, information exchange and recognition of digital credentials across various jurisdictions. However, these efforts are not sufficient because the problems cannot be limited to a region or subregion. Efforts to establish appropriate national organizational structures and link them together through international cooperation are indispensable to provide global solutions to these global issues.

Capacity building: What you don't know will hurt you

In cybersecurity, people are the weakest link. People are the users, they develop the systems, they elaborate the policies and they put in place the strategies and procedures. Capacity building and a high level of awareness is therefore one of the principal challenges we face today.

Like anyone using any modern infrastructure such as roads, children surfing in a cybercafé need basic awareness on how to safely benefit from the potential of ICTs while avoiding some of the dangers. They need to be aware of the dangers linked to not knowing whom they are dealing with. They need to be aware of the potential dangers of revealing personal information such as their name, telephone number and address to cyberhawks who pretend to be children and lure them to physical meetings.

Governments have to draw up policies and strategies to meet their developmental targets and for national security purposes. Policy-makers and regulators need to be aware of the dangers related to the modification of sensitive medical data or the unauthorized access to such systems. Legislators must have basic knowledge of how legal instruments map to existing technological solutions in place.

With the important role that ICTs play today in protecting critical infrastructure and providing services in sectors such as health, education, finance and commerce, knowledge and know-how on the opportunities offered by a secure cyberspace and on the threats inherent in an insecure cyberspace are vital to meeting national priorities. Inadequate and inappropriate programmes for capacity building on the basics of cybersecurity technologies and strategies for engineers, internet service providers and network operators who run and operate the networks and IT infrastructure could pose severe threats in an environment where networks and host are interconnected and form a borderless and global infrastructure. It is often said that a chain is as strong as its weakest link and, in an era of global connectivity, it is important that this connectivity should also extend to knowledge and know-how.

Programmes aimed at creating a level playing field in raising basic awareness and building capacity need to be undertaken within the framework of international cooperation.

International cooperation

This is a global problem and it needs a global solution

These issues are global. Countries cannot shut down their borders to incoming cyberthreats. Cybercriminals are not and cannot be bound to geographical locations. Laws and technological measures can no longer be limited to national or regional boundaries. Time and geography are no longer barriers to where and when these attacks can be launched and where the victims could be located. Attempts to try to solve these challenges at the national or regional levels are simply not sufficient. Legal and technical measures operating at national and regional levels are necessary but not sufficient to address these global challenges.

Understanding what cybersecurity means to all

To put in place a global solution to address these challenges, it is first of all important that all countries arrive at a basic common understanding of what cybersecurity means to them. cybersecurity is basically about providing protection against unauthorized access, manipulation and destruction of critical resources and assets. These resources and assets, and the related issues to be addressed, vary and depend on the level of development of countries. They also depend on what they consider to be a critical resource, the efforts they are willing and able to make and their assessment of the risks they are willing to accept as a result of inadequate cybersecurity measures.

Many least developed countries consider cybersecurity primarily as a means to extend the benefits of ICTs through the delivery of secure and high-trust services in sectors such as health, commerce, public administration and finance. Their needs, priorities and strategies in cybersecurity are not necessarily the same as those of the most developed countries. However, quite a number of developed countries, in addition to other threats such as online fraud, consumer protection and privacy, also consider cybersecurity solutions as a way to protect and maintain the integrity of critical infrastructures in the financial, health, energy, transportation, telecommunication, defence and other sectors. Critical Information Infrastructure Protection, or CIIP, is therefore quite high on the agenda of many developed countries.

b A global strategy for action and the role of ITU

With an estimated one billion people connected to the Internet from all countries in the world and different levels of development, priorities and challenges, it is obvious that global issues such as cyberthreats and inadequate cybersecurity solutions could be seen differently by different countries.

With its 191 Member States and more than 700 Sector Members, ITU is uniquely placed to put in place a framework for international cooperation in cybersecurity. Its membership includes the least developed, developing, emerging economies and the industrialized countries. ITU therefore provides a forum where these diverse views of what cybersecurity and cybercrime mean to various countries can be discussed, with the goal of arriving at a common understanding amongst countries on those issues that are common to all countries and how they could be addressed globally. Its lead role as moderator/facilitator for WSIS Action Line C5, its mandate in the standardization and development domains of cybersecurity, and having cybersecurity as one of its high priority activities and as a long-term strategic goal provide a unique opportunity to the global information society as a forum for designing and implementing solutions aimed at addressing these global challenges.

The strategy for a solution must identify those existing national and regional initiatives, work with all relevant players to avoid duplication and put in place strategies for bringing together partners and initiatives with the goal of proposing global solutions to address the global challenges we are facing today.

The global nature of the legal, technical, operational, organizational and policy challenges requires synergies with existing initiatives, multi-stakeholder partnerships and global coordination. Working with interested and relevant partners on issues where a common understanding has been reached is the only way we can address these global issues and build a secure and high-trust information society for all nations and peoples.

Together with partners from governments, industry, international organizations and civil society, ITU is proposing a global framework for international cooperation aimed at providing concrete measures and solutions to enhance security and confidence in the information society.

The Global Cybersecurity Agenda (GCA) will build on existing initiatives and partners with the objective of proposing solutions to address some of the challenges faced today in cybersecurity and cybercrime. The ultimate objective of the Cybersecurity Agenda is to make significant progress on the agreed goals in the fight against cybercrime and increase the level of confidence and security in the information society. It will be based on international cooperation, and will strive at getting the engagement of all relevant stakeholders in a concerted and coordinated effort to make a difference and to build security and confidence in the information society.

c ITU framework

- **Vision of ITU Secretary-General** – To create a secure and high-trust information society for all nations where all participants of the global information society can reap the benefits of ICTs and avoid the dangers and pitfalls.
- **Resolution 130 (revised Antalya, 2006)** – Strengthening the role of ITU in building confidence and security in the use of ICTs:
  Instructs the Secretary-General and the Directors of the Bureaux to: Facilitate access to tools required for enhancing confidence and security in the use of ICTs for all Member States, consistent with WSIS provisions on universal and non-discriminatory access to ICTs for all nations.
- **Relevant ITU Resolutions and decisions on cybersecurity** – Resolution 130 (revised Antalya 2006), Doha Action Plan Programme 3, WTSA Resolutions 50, 51 and 52.
- **ITU responsibility related to WSIS implementation** – Maintaining and further promoting a leadership role for ITU as the main facilitator for WSIS Action Line C5, Building confidence and security in the use of ICTs.

An overview of the strategy for moving forward on international cooperation in cybersecurity

1 The framework for international cooperation and domains for the identification of the items of the Global Cybersecurity Agenda are the following:

a) Legal Aspects

b) Technical Measures

c) Organizational Structures (including Policies and Strategies)

d) Capacity Building (cross-cutting and covering **a)** to **c)** above)

e) International Cooperation (cross-cutting in **a)** to **d)** above)

2 In putting together this framework, ITU strategy is to work with all relevant partners to identify the challenges and propose solutions and strategies to address existing challenges and better understand emerging and future threats in cybersecurity.

3 Ensure the full engagement of all countries (least developed, developing, transitional and industrialized) in working towards the solutions and goals identified.

4 Establish a global framework for international cooperation on cybersecurity – to propose concrete solutions as items of the Global Cybersecurity Agenda.

d The ITU Global Cybersecurity Agenda

The challenges to be addressed in building global security and trust span across several work areas (e.g. technologies, policies and strategies, legislation, capacity building, enforcement and others). The Global Cybersecurity Agenda is a set of defined challenges in five (5) broad domains, and of proposed solutions aimed at addressing these challenges within a framework of international cooperation and in collaboration with all relevant stakeholders. It focuses on those cross-cutting and global challenges in the Legal, Technical, Organizational, Capacity Building and International Cooperation domains. In developing the items that make up the Agenda, emphasis will be on leveraging expertise from the relevant players and taking account of existing initiatives.

Within ITU, the Global Cybersecurity Agenda is aimed at complementing the work being undertaken by ITU-D and ITU-T to avoid duplication and overlaps, and will propose solutions and strategies that will facilitate the implementation of BDT programmes and projects in developing countries. It would also enhance the work of ITU-T through proposals for new areas for standards development and collaboration with other entities involved in cybersecurity-related standards.

The Global Cybersecurity Agenda goes beyond listing the tasks to be done or the challenges to be faced. Rather, it proposes strategies and solutions developed with the support and participation of relevant stakeholders, while taking account of existing initiatives.

The initial items of the Global Cybersecurity Agenda

Central to the elaboration of items of the Agenda is the establishment of a High-Level Experts Group (HLEG) as one of the main instruments for refining the broad goals listed in points **1**-**7** below, and for identifying emerging trends in cybersecurity, as well as developing proposals for future ITU work to address current and emerging cybersecurity challenges and formulating proposals in the form of solutions to meet these goals.

1. Development of *model cybercrime legislation* that is globally interoperable with existing national and regional initiatives and putting in place a framework for global cooperation among interested countries.

2. Development of a strategy for the establishment of globally accepted minimum security *criteria and accreditation schemes for software applications and systems* through cooperation with existing national and regional public and private sector initiatives.

3. Creation and endorsement of a *generic policy model* and *national strategies* for the establishment of appropriate national and regional organizational structures to deal with cybercrime.

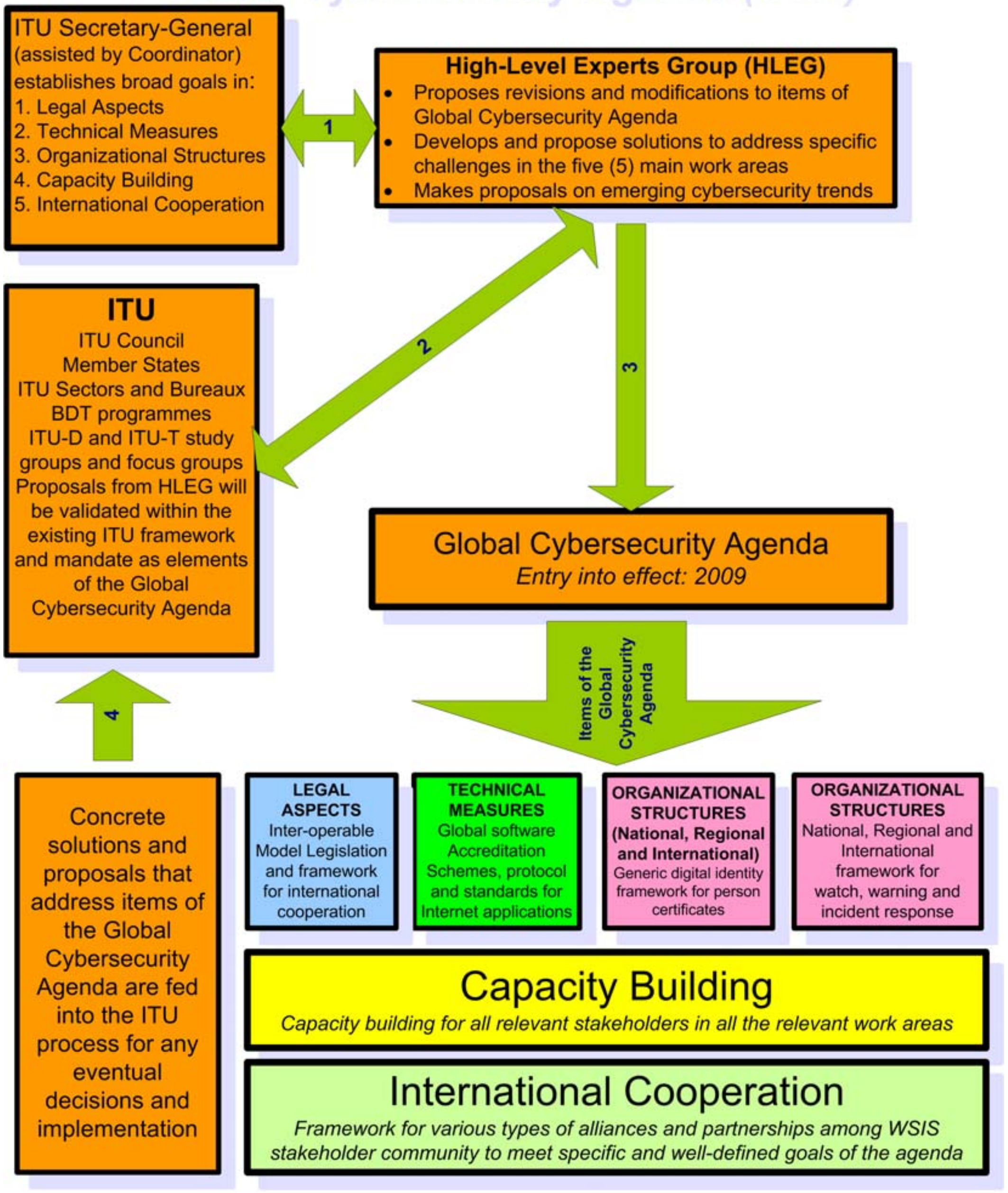
4. Establishment of a framework for *watch, warning and incident response* to ensure global cooperation between new and existing initiatives.

5. Creation and endorsement of a *universal generic identity framework* and necessary organizational structures to ensure the recognition of digital credentials for citizens across geographical boundaries.

6. Development of a *global strategy to facilitate human and institutional capacity building* to enhance knowledge and know-how across the sectors and amongst the players.

7. Establishment of a *global multi-stakeholder strategy* and framework for international cooperation and collaboration in all the above-mentioned areas.

Overview of the
Global Cybersecurity Agenda (GCA)



ITU Secretary-General (assisted by Coordinator) establishes broad goals in:
1. Legal Aspects
2. Technical Measures
3. Organizational Structures
4. Capacity Building
5. International Cooperation

High-Level Experts Group (HLEG)
- Proposes revisions and modifications to items of Global Cybersecurity Agenda
- Develops and propose solutions to address specific challenges in the five (5) main work areas
- Makes proposals on emerging cybersecurity trends

ITU
ITU Council
Member States
ITU Sectors and Bureaux
BDT programmes
ITU-D and ITU-T study groups and focus groups
Proposals from HLEG will be validated within the existing ITU framework and mandate as elements of the Global Cybersecurity Agenda

Global Cybersecurity Agenda
Entry into effect: 2009

Concrete solutions and proposals that address items of the Global Cybersecurity Agenda are fed into the ITU process for any eventual decisions and implementation

LEGAL ASPECTS
Inter-operable Model Legislation and framework for international cooperation

TECHNICAL MEASURES
Global software Accreditation Schemes, protocol and standards for Internet applications

ORGANIZATIONAL STRUCTURES (National, Regional and International)
Generic digital identity framework for person certificates

ORGANIZATIONAL STRUCTURES
National, Regional and International framework for watch, warning and incident response

Capacity Building
Capacity building for all relevant stakeholders in all the relevant work areas

International Cooperation
Framework for various types of alliances and partnerships among WSIS stakeholder community to meet specific and well-defined goals of the agenda

Details on activities related to the implementation of specific tasks to meet the goals set in the Agenda and the required partnerships and alliances are not covered in this diagram. Cooperation with existing national and regional initiatives and close collaboration within ITU will be vital for implementation to avoid duplication, build the necessary synergies and for the efficient use of existing and limited resources.

Establishment of a High-Level Experts Group (HLEG)

Vital for the development of the Global Cybersecurity Agenda and in its implementation is the formation of a multi-stakeholder High-Level Experts Group with an advisory capacity. The main responsibilities of the HLEG include:

1 Main responsibilities

- In close collaboration with ITU and in consultation with the Secretary-General, propose refinements to and review of the initial items of the Global Cybersecurity Agenda. This will lead to a decision on the items for which efforts must be made in developing proposals and solutions.
- Develop and propose concrete solutions aimed at facilitating the achievement of well-defined ITU strategic goals that are items in the Global Cybersecurity Agenda.
- Provide support and assistance in facilitating the implementation of items in the Global Cybersecurity Agenda within the framework of ITU's mandate in cybersecurity.
- Provide technical information and knowledge and expertise on the different areas of cybersecurity in the form of written contributions.
- Provide advice on possible long-term strategies and emerging trends in cybersecurity for consideration by the appropriate ITU forum for future work programmes.

2 Composition

The main purpose of the High-Level Experts Group is to use recognized sources of expertise in order to develop and propose practical solutions to facilitate the achievement of well-defined ITU strategic goals in cybersecurity. Some features and characteristics of the HLEG include the following:

- A multi-stakeholder global think-tank comprising leading industry players, governments, relevant regional/international organizations, research and academic institutions and individual experts.
- Organizations, countries and industry will be represented by senior officials (Ministers, CEOs and heads of organizations).
- Membership of the High-Level Experts Group will be appointed by the ITU Secretary-General, taking account of members' expertise in the five (5) work areas (Legal Aspects, Technical Mesures, Organizational Structures, Capacity Building and International Cooperation).

- Each member entity of the HLEG will designate experts to work on specific areas (Working Groups) based on the expertise of that entity.
- The HLEG will be operational for the duration of two years, with the possibility of renewal.
- The group will have 50 high-level members, with the following composition:
  1 Member States (10) – two countries per ITU region

  2 Industry (20) – striving towards regional balance

  3 International organizations (5)

  4 Academic and research institutions (5)

  5 Civil society (5)

  6 Individual experts (5)

3 Working groups

The HLEG will consist of five (5) working groups:

1 Legislative Working Group

2 Technology Working Group

3 Organizational (including Policies and Strategies) Working Group

4 Capacity Building Working Group (Cross-cutting)

5 International Cooperation Working Group (Cross-cutting)

4 Working methods, funding and collaboration within ITU

a The work of the High-Level Experts Group will be funded primarily through voluntary contributions from its members and other interested parties.

b ITU will provide the facilities and secretarial support for the HLEG and will host two annual physical meetings in Geneva where HLEG will present its biannual progress report on proposals to address the challenges in the Agenda.

c The High-Level Experts Group is to be assisted by the ITU Coordinator to ensure that the proposals are consistent with ITU's mandate and ITU's role as moderator/facilitator for WSIS Action Line C5.

d Some proposals and solutions developed by the HLEG will be submitted for refinement, validation and eventual decisions for implementation by the relevant ITU Sectors.

e Expertise from existing and relevant ITU structures, including ITU Bureaux, ITU-T and ITU-D study groups, and specific focus groups, will also be used to review proposals in accordance with the ITU Constitution/Convention, to enable their implementation.

f Refined and validated proposals will be confirmed as definitive items in the Cybersecurity Agenda. This is to ensure that all items in the Global Cybersecurity Agenda can be implemented by ITU with the support of partners, Member States and other interested and relevant stakeholders.

g The HLEG is expected to complete its work in two years from the date of entry into effect of the Group.

e-mail: gca@itu.int
www.itu.int/cybersecurity/gca