International Telecommunication Union

ITU Global Cybersecurity Agenda (GCA)

A Framework for International Cooperation in Cybersecurity

International Telecommunication Union

Foreword to the ITU Global Cybersecurity Agenda

The power of the virtual world increases every day. By the time your eyes reach the end of this page, that power will have grown even further. A young student in a developing country will have accessed the library of a prestigious university; a senior citizen who has never travelled abroad will have visited a nation on the other side of the world; a small-business owner will have attended an international conference without leaving her office. With each of these achievements, the virtual world brings about another real-world victory for education, dialogue, and better understanding between peoples.

Unfortunately, there is nothing virtual about the hazards that accompany modern communications technologies. The Internet may open our minds to new possibilities, but it also exposes us to the pitfalls and dangers of online predators. What's more, like so many of the challenges facing our planet today, these dangers know no borders. Just as viruses and bacteria can spread unchecked from region to region, computer viruses spread from computer to computer, regardless of location. Just as crime and violence in one country affect life in another by sending streams of displaced refugees seeking relief, cybercrime in one nation can find victims anywhere. Just as pollution and destruction in one area can cause climate change on a global level, child pornography from a single source pollutes minds around the world.

We have a vital responsibility to ensure the safety of all those who venture online – especially as online services become a more integral part of citizens' lives. Technology is improving direct and democratic access to health, financial and telecommunications services, among many others. None of us would stand idly by during attacks or theft at the hospital or bank or phone company; we must provide the same security to the increasing number of people who work with these institutions online. Leaders strive to ensure the safety of their citizens on their countries' highways and roads; the attention to safety on the information superhighway, where people young and old travel for hours each day, should be no different.

The world must take action, and it must stand united. This is not a problem any one nation can solve alone. A global framework is needed, giving us international principles to match hackers' international range, and allow rapid coordination between countries at the regional and global levels. The Global Cybersecurity Agenda represents such a framework, and I am proud that International Telecommunication Union Secretary-General Hamadoun Touré has invited me to serve as a patron of this important effort.

I have spent my life working for education and peace. The free exchange of ideas and information online has tremendous power to support both of these goals. However, threats to online security endanger that potential. I invite you to join with me in supporting ITU's urgent effort – because by the end of this page, by the end of this day, peace and safety in the virtual world will become an ever more essential part of peace and safety in our everyday lives.

Dr Óscar Arias Sánchez
President of the Republic of Costa Rica,
Nobel Peace Prize Laureate

Foreword

With more than a billion people connected to the Internet, information and communication technologies (ICT) are the driving force for today's economic growth. They are also the most important tools to meet 2015 targets of the Millennium Development Goals. However, the misuse of these advances in technology, along with the absence of truly global and multi-stakeholder strategies to address the global challenges we face, are threatening the collective benefits we as citizens of the information society should obtain.

Cybersecurity and cyberpeace are the most critical concerns of our information age. Criminals are on the prowl to prey on the unwary and use their technical skills to break into networks not only for financial gain but also to collect information, invade privacy, steal identities, sow hatred and, worst of all, pander to the nefarious habits of paedophiles. Financial loss alone is estimated to run into several billion dollars both from fraud on the Internet and from the costs of rebuilding networks that have suffered cyberattacks. Moreover national security can be at risk if hostilities and extremism are taken into cyberspace.

Making a simple transaction on the Internet using a credit card can be fraught with danger. Imagine the difficulties this could pose in an increasingly networked world of e-commerce and e-government. Hackers can thwart sophisticated banking systems. Children, students and senior citizens communicating by Internet or mobile phone are equally vulnerable. A patient could lose his life if the medical files are tampered with.

We must act now to deal with this menace. Unless there is close international cooperation, even countries with strong cybersecurity measures in place will be at risk because they will not be able to prosecute criminals outside their national or regional jurisdictions.

The World Summit on the Information Society, which concluded in Tunis in November 2005, asked ITU to coordinate a mechanism for building confidence and security in the use of ICTs. The International Telecommunication Union provides the global perspective and expertise needed to meet the challenges, with a track record of brokering agreements between public and private interests on a level playing field ever since its inception in 1865.

I launched the Global Cybersecurity Agenda on World Telecommunication and Information Society Day 2007 and I am honoured that Dr Óscar Arias Sánchez, Nobel Peace Prize Laureate and President of the Republic of Costa Rica, has accepted to be the Patron of this initiative.

Dr Hamadoun I. Touré
Secretary-General
International Telecommunication Union

Overview

Confidence and security in using ICTs are fundamental in building an inclusive, secure and global information society. Confidence and security are vital in the effective use of ICTs, as acknowledged by the World Summit on the Information Society (WSIS).

The legal, technical and institutional challenges posed by cyberattacks and cybercrime are global and far-reaching, and can only be addressed through a coherent strategy taking into account the role of different stakeholders and existing initiatives, within a framework of international cooperation.

Current attempts to address these challenges at the national and regional levels are inadequate, as cyberspace is boundless and limited only by human imagination. The boundaries of the information society have no direct correlation with existing geographical borders – cyberthreats can arise anywhere, at any time, causing immense damage in a very short space of time, before they are tackled.

The WSIS recognized the real and significant risks posed by cybercrime and entrusted ITU with facilitating 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 countries, developing and emerging economies, as well as developed countries. ITU is therefore an excellent forum where actions and responses to promote cybersecurity and tackle cybercrime can be discussed, with the goal of arriving at a common understanding as to how best these challenges can be addressed.

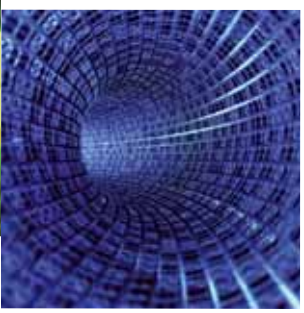
The Global Cybersecurity Agenda (GCA) is an ITU framework for international cooperation aimed at proposing strategies for solutions to enhance confidence and security in the information society. It will build on existing national and regional initiatives to avoid duplication of work and encourage collaboration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

Constant evolution of the nature of cyberthreats

Cyberthreats have become increasingly sophisticated since the early 1980s, when the first known case of a computer virus was reported. As recently as a few years ago, the development of malware (including viruses, worms and Trojans) presented a simple intellectual challenge to information technology (IT) experts to demonstrate their technical skills. Today, cybercrime has become an organized syndicate reaping financial rewards and using diverse tools to threaten different platforms in various countries. No country is safe. Spam has evolved to become a vehicle disseminating other dangerous malware to perpetrate online financial fraud, identity or trade-secret theft, among other risks. Taking into account newer threats to critical infrastructure in the financial, health, energy, transportation, telecommunication, defence and other sectors, the impact of cyberthreats is becoming ever greater. Further, the risks are evolving in line with the technologies. For example, one emerging menace is the shift in strategy by hackers from a central command-and-control model for controlling botnets to a peer-to-peer model with a distributed command structure, capable of spreading to compromised computers located in different countries. This practice makes it very difficult to pinpoint any single geographical location as the origin of cyberattacks using botnets, and consequently makes it more difficult to identify them and shut them down. This shift in strategy is not just aimed at delivering courier spam and malware, 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 barriers and increasing sophistication of cybercrime

Toolkits and applications for phishing, spam, malware, scareware and snoopware can today be acquired relatively easily from underground sites or even purchased legally, lowering the financial and intellectual entry barriers to acquiring tools to facilitate unauthorized access to information and communication systems to manipulate or destroy them.



Snoopware is going mobile, threatening user privacy through the possibility of voice/data call monitoring, with 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 telephony (including smartphones), together with convergence, which is bringing down the walls between networks, cyberthreats can now spread easily to all platforms and to all countries .

As information technology becomes an ever greater part of our lives, and as ubiquitous connections to the Internet become a reality, with computers integrated into a growing number of household appliances, it is increasingly likely that cyberthreats will spread to new levels and affect us in ways unimaginable today.

Loopholes in current legal frameworks

Cybercriminals are already exploiting vulnerabilities and loopholes in national and regional legislation. There is evidence that they are shifting their operations to countries where appropriate and enforceable laws are not yet in place, so that they can launch attacks on victims with almost total impunity, even in those countries which do have effective laws in place.

With the spread of networks of hijacked computers over different countries, criminals can launch cyberattacks using a decentralized model based on peer-to-peer arrangements, making it difficult for any single national or regional legal framework to deal adequately with this problem. Such far-reaching challenges can only be addressed at the global level.

Many countries have adopted or are working on legislation to combat cybercrime and other misuses of information technology. These laws are drawn up so as to be enforceable in well defined geographical boundaries that are either national or regional. However, even if all countries introduce legislation, cybercriminals cannot be easily extradited between the country where the cybercrime was instigated and the country where it was committed, unless these legal frameworks are inter-operable. This is far from the case today.

Some efforts to address this challenge have been undertaken, by establishing bilateral agreements and memoranda of understanding between countries. However, bilateral agreements may be limited in their scope and effectiveness, due to the complexities involved in negotiating numerous bilateral agreements based on different terms and conditions. Further problems arise, where countries may need to extend such agreements to various others countries. A strategy based on cooperation through bilateral agreements may also result in differences in agreed responsibilities – for example, where, say, five countries are signatories to 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 – although valuable – are not the solution to the tackle the far-reaching legal challenges we face today in dealing with cyberthreats. At best, they may only shift the problem from one country to the next and result in creating cybercrime-havens for cybercriminals who are protected by the extraterritoriality of their activities.

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 communication systems. Just as access to information is enhanced by the borderless nature of the information society, so too 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 enough is being done to address the shortfall of applications on which many users rely for the delivery of critical services, in domains such as health, finance, commerce and public administration.

For developing countries that rely on ICT applications to enhance access to basic services (such as e-health, e-government and e-commerce), the threats posed by the exploitation of software vulnerabilities in order to gain unauthorized access and control of information systems cannot be overestimated. Such access 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 under way to address the challenges related to standardizing accreditation for software applications in order to reduce their vulnerabilities and make access to the information society more secure. Such efforts focus mainly on security applications and devices. They need to be extended to normal applications. It is vital to leverage the experience of the software and hardware security industry and take account of existing initiatives and expertise to design strategies within a framework of international cooperation. Accreditation schemes, protocols and standards must also be put in place to address the security vulnerabilities exploited today by cybercriminals to gain access and control to information systems and data.

Absence of appropriate organizational structures

The absence of institutional structures to deal with incidents (such as virus and network attacks resulting in fraud, the destruction of information and/or the dissemination of inappropriate content) is also a genuine problem in responding to cyberattacks.

While some countries and regions have set up agencies dealing with watch and warning systems and incident response, and have put in place the organizational structures for coordinating responses to cyberattacks, much more still needs to be done. When a cyberattack occurs in one country, its devastating effects can reach victims in connected countries in a matter of minutes. The free flow of information, collaboration and cooperation between national organizational structures are vital to deal effectively with and respond to such incidents.

Another area where it is necessary to establish organizational structures and appropriate policies is in the domain of generic identity certificates (digital certification). User authentication has long been recognized as a vital strategy in combating cyberthreats (identity theft, phishing and other forms of online fraud). Strong authentication is a key component for building confidence and security in the information society. While some countries have established the organizational structures and infrastructure needed to provide generic identity certificates to citizens, such structures have yet to be established in other countries. A global framework is needed 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 the recognition of digital credentials across different jurisdictions.

However, these efforts are currently insufficient, because such problems are not limited to any single region or subregion. Efforts to establish appropriate national organizational structures and link them together through international cooperation are indispensable in providing global solutions to these global challenges.

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 to secure transactions. Capacity building and a high level of user awareness is thus one of the key challenges we face today.

Like any user of modern infrastructure such as roads, children surfing in a cybercafé need a basic awareness of how to benefit from ICTs safely, whilst avoiding some of the dangers. They need to be aware of the dangers associated with not knowing whom they are dealing with. They need to be aware

of the risks of revealing personal information (including their name, telephone number and address) to cyberhawks, who may pretend to be children and lure them towards a physical meeting.

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

With the important role that ICTs play today in providing services in sectors as varied as health, education, finance and commerce, awareness of the opportunities offered by a secure cyberspace and of the threats inherent in an insecure cyberspace are vital to meeting national priorities. More active programmes for capacity building on the basis of cybersecurity and strategies for engineers, Internet Service Providers and network operators who run and operate the networks and IT infrastructure would help enhance a networked environment

where networks and host are interconnected to form a borderless and global infrastructure. It is often said that a chain is only 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: Cyberthreats are a global problem and they need a global solution

Cyberthreat issues are global. Countries cannot easily close their borders to incoming cyberthreats. Time and geography, as well as the location of victims, are no longer barriers to where and when these attacks are launched by cybercriminals. Attempts to try to solve these challenges at the national or regional levels have proven insufficient. Legal and technical measures at the national and regional levels are necessary, but not sufficient, to address these global threats.

Understanding what cybersecurity means to all

To put in place a global solution to address those challenges, it is vital that all countries arrive at a common understanding of what cybersecurity means. Cybersecurity is about providing protection against unauthorized access, manipulation and destruction of critical resources and assets, such as data.

The value of these resources and assets varies from country to country and depends in part on the level of development and type of economic activities. Their value also depends on what each country considers to be its critical resources, the efforts it is willing and able to make and its assessment of the risks that it is willing to accept, in a trade-off with the cybersecurity measures that it is prepared to implement.

Many least developed countries consider cybersecurity mainly 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 their critical infrastructures in the financial, health, energy, transportation, telecommunication, defence and other sectors. Critical Information Infrastructure Protection (CIIP) is thus high on the agenda of most, if not all, countries.

A global strategy for action and the role of ITU

With an estimated one billion people currently using the Internet around the world, it is understandable that global issues such as cyberthreats and inadequate cybersecurity solutions can be viewed differently by countries with dissimilar levels of development, priorities and challenges.

With its 191 Member States and more than 700 Sector Members and Associates, ITU is uniquely placed to seek consensus on a framework for international cooperation in cybersecurity. Its membership includes the least developed countries, the developing and emerging economies and the industrialized countries. ITU, therefore, provides the preeminent forum where the diverse views about cybersecurity and cybercrime, including those of the private sector, can be discussed, with the goal of arriving at a common understanding amongst all the concerned parties and how those issues could be addressed globally and effectively.

Moreover, the known mandate of ITU in the standardization and development of telecommunications was recognized when world leaders appointed ITU as moderator/facilitator for WSIS Action Line C5. This acknowledgment reinforces ITU as an ideal forum for developing and putting into action solutions aimed at addressing the global challenges to cybersecurity.

The strategy for a solution must identify those existing national and regional initiatives, work

with all relevant players to identify priorities and bring partners together with the goal of proposing global solutions to address the global challenges we face today.

Working with key partners on issues where a common understanding can be reached is the only way to address these global issues and build a safe and secure information society for all nations and peoples.

Alongside partners from governments, industry, relevant regional/international organizations, research institutes, academic institutions and individual experts, ITU has therefore established a global framework for dialogue and international cooperation aimed at proposing strategies for solutions to enhance security and confidence in the information society. The Global Cybersecurity Agenda (GCA) will unite existing initiatives and partners with the objective of proposing global strategies to address today's challenges in the fight against cybercrime and to maintain cyberpeace. The ultimate aim of the Global Cybersecurity Agenda is to make significant progress on the agreed goals in the fight against cybercrime and to increase the level of confidence and security in the information society. It is based on international cooperation, and strives to engage all relevant stakeholders in a concerted effort to build security and confidence in the information society.

A unique vision
A unique forum

The ITU Secretary-General has identified cybersecurity as a top priority. The **Secretary-General's vision** is a global information society in which trust and security in the use of ICTs is the norm, and in which each and every participant can reap the benefits and opportunities afforded by ICTs.

WSIS implementation

At the second phase of the World Summit on the Information Society (WSIS) in Tunis in 2005, ITU was entrusted to take the lead as the sole facilitator for **Action Line C5,** "Building confidence and security in the use of information and communication technologies (ICTs)".

Calls from ITU membership

In line with these developments, ITU membership has been calling for a greater role to be played by ITU in matters relating to cybersecurity through various **Resolutions, Decisions, Programmes and Recommendations:**

- **Resolution 71 of the ITU Plenipotentiary Conference (Antalya, 2006)**
  This Resolution outlines the Strategic Plan for the Union for 2008-2011, including its mission and nature, strategic orientations and goals and detailed objectives for the Sectors. Under Goal 4, ITU should specifically engage in "developing tools, based on contributions from the membership, to promote end-user confidence, and to safeguard the efficiency, security, integrity and interoperability of networks", with information and communication network efficiency and security defined as including, *inter alia*, spam, cybercrime, viruses, worms and denial-of-service attacks. Under Objective 3, ITU's General Secretariat has been tasked to facilitate the internal coordination of activities among the three Sectors where work programmes are overlapping or are related, so as to assist the membership in ensuring that it benefits from the full complement of expertise available within the Union.
- **Resolution 130 of the ITU Plenipotentiary Conference (Revised, Antalya, 2006)**
  "Strengthening the role of ITU in building confidence and security in the use of information and communication technologies"
- **Doha Action Plan Programme 3 of the ITU World Telecommunication Development Conference (Doha, 2006)**
  "E-strategies and ICT applications"
  "Cybersecurity: Enhance security and build confidence in the use of ICT applications"
- **Resolution 2 of the ITU World Telecommunication Development Conference (Doha, 2006)**
  Annex 2 of Resolution 2 resolves that Study Group 1 will study Question 22/1 "Securing information and communication networks: best practices for developing a culture of cybersecurity"

- **Resolution 50 of the ITU World Telecommunication Standardization Assembly (Florianópolis, 2004)**
  "Cybersecurity"
- **Resolution 149 of the ITU Plenipotentiary Conference (Antalya, 2006)**
  "Study of definitions and terminology relating to building confidence and security in the use of information and communication technologies"
- **ITU-T Recommendation X.509**
  "Public-key and attribute certificate frameworks (global standard on identity management)"
- **ITU-T X.8xx Series Recommendations**
  Global standards on key security aspects including authentication, access control, non-repudiation, confidentiality, integrity, audits and security architecture for systems providing end-to-end communications.
- **ITU-T Recommendation X.805**
  "Security architecture for systems providing end-to-end communications"
- **ITU-T Recommendation X.811**
  "Information technology – Open Systems Interconnection – Security frameworks for open systems: Authentication framework"
- **ITU-T Recommendation X.812**
  "Information technology – Open Systems Interconnection – Security frameworks for open systems: Access control framework"
- **ITU-T Recommendation X.1051**
  "Information security management system – Requirements for telecommunications (ISMS-T)"
- **ITU-T Recommendation X.1121**
  "Framework of security technologies for mobile end-to-end data communications"
- **Resolution 45 of the ITU World Telecommunication Development Conference (Doha, 2006)**
  "Mechanisms for enhancing cooperation on cybersecurity, including combating spam"
- **Resolution 51 of the ITU World Telecommunication Standardization Assembly (Florianópolis, 2004)**
  "Combating spam"
- **Resolution 52 of the ITU World Telecommunication Standardization Assembly (Florianópolis, 2004)**
  "Countering spam by technical means"
- **ITU-R Recommendation M.1457**
  "Security mechanisms incorporated in IMT-2000"
- **ITU-R Recommendation S.1711**
  "Performance enhancements of transmission control protocol over satellite networks"
- **ITU-R Recommendation M.1645**
  "Framework and overall objectives of the future development of IMT-2000 and systems beyond IMT-2000"
- **ITU-R Recommendation M.1223**
  "Evaluation of security mechanisms for IMT-2000".
- **ITU-R Recommendation S.1250**
  "Network management architecture for digital satellite systems forming part of SDH transport networks in the fixed-satellite service "
- **ITU-R Recommendation M.1078**
  "Security principles for IMT-2000"

An Agenda for change
A global strategy

Five pillars of the ITU Global Cybersecurity Agenda

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

1 Legal Framework

2 Technical 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 cross-border 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 in-kind) from its members and other donors.

1 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.

2 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

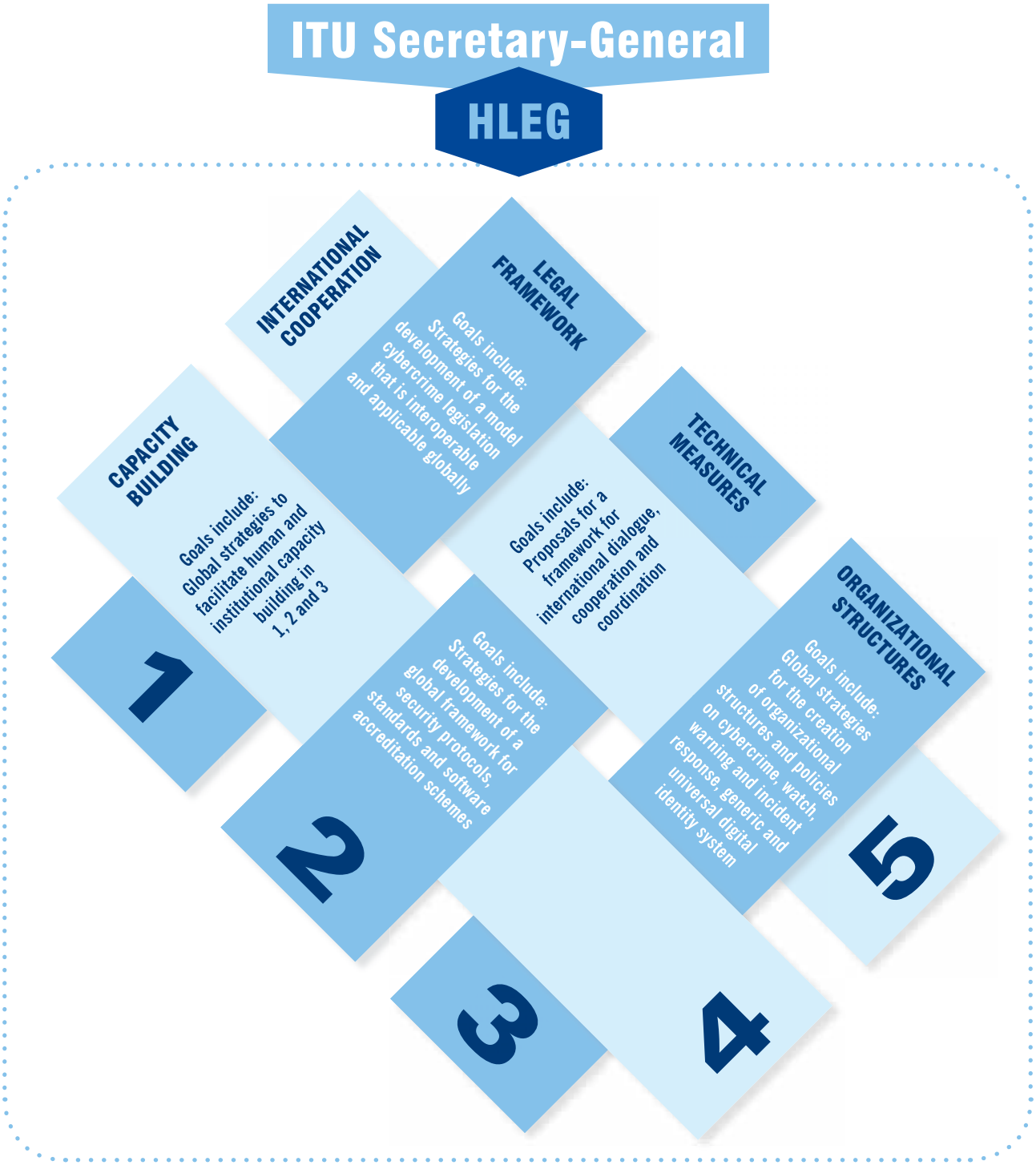
c Regional/International organizations

d Research and academic institutions

e Individual experts

GLOBAL CYBERSECURITY AGENDA

A FIVE-PART PLATFORM



Global Cybersecurity Agenda

International Telecommunication Union
Corporate Strategy Division
Place des Nations
CH-1211 Geneva 20

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

09-2007 – Photo credits: iStockphoto