CONTENT

FOREWORDS

Dr Hamadoun I. Touré,
ITU Secretary-General

Information and Communication Technologies (ICTs) have transformed modern lifestyles. These have provided us with real-time communications, borderless and almost unlimited access to information and a wide range of innovative services. At the same time, these have also created new opportunities for exploitation and abuse.

Cyber threats have become one of the biggest global issues of our time. The proliferation of always-on connections has created a global network of open conduits. Whilst this brings untold benefits in terms of access to information and knowledge on an unprecedented scale, it has also led to vast quantities of malware and spyware circulating freely on the Internet, and an alarming rise in the number and scale of cyber threats, cyber criminals and cyber terrorists.

ITU has been working hard to forge partnerships and support projects whose goal is to create a safe and secure cyber environment for everyone. Access to communications is useless if peace and safety online cannot be guaranteed.

That is why the ITU, as facilitator of WSIS Action Line C5 on "Building Confidence and Security in the use of ICTs", launched the Global Cybersecurity Agenda (GCA) on 17 May 2007. Designed as an international framework for cooperation and response, the GCA focuses on building partnership and collaboration between all relevant parties in the fight against cyber threats.

Cybersecurity is one of the most critical concerns of the information age. It forms the cornerstone of a healthy, connected world. It is a global issue, demanding a truly global approach. Because of light-speed communications and ubiquitous networks, cyber criminals and cyber terrorists do not need to be anywhere near the scenes of their crimes. An international response is the only answer and possible solution.

It is therefore gratifying to see, and to be part of, this growing coalition aimed at building global solutions to address cyber threats whatever the source. I am convinced that the ITU, based on its expertise, can build confidence and trust in the use of ICTs to make the online world a safer place.


IMPACT
INTERNATIONAL MULTILATERAL PARTNERSHIP AGAINST CYBER
Media Confer
20 March 2009
IMPACT

H.E. Dr Arias, former President of Costa Rica and Nobel Peace Prize winner, Patron of the 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.

H.E. Mr. Compaoré President of Burkina Faso, Patron of the Global Cybersecurity Agenda

Information and communication technologies (ICTs) play a decisive role in the development process. In order to take full advantage of all the opportunities, the time has therefore come to establish solid foundations more conducive to bringing about the desired economic growth.

In Africa, and indeed worldwide, ever-increasing numbers of people are using ICTs and the services they enable. It is therefore both desirable and necessary to provide them with a safe and secure cyber environment.

This is the main reason why I am pledging my personal support, and agreeing to serve as a patron, for the Global Cybersecurity Agenda, initiated by the International Telecommunication Union (ITU). Given the interdependencies that are created by information and communication technologies, I appeal to Member States to be unstinting in their commitment to ensuring the success of the Agenda as an appropriate framework for cooperation.

Countries must focus their political responsibility and spare no effort on developing agreements that are sufficiently effective and flexible to stem cybercrime.

It is in this spirit that Burkina Faso will make its contribution to ensuring full realization of the Global Cybersecurity Agenda in the interests of making the world a safer place.

For my part, I will give all the necessary time and support to this undertaking, confident as I am of the backing of my African peers and the international community.

INTRODUCTION

Today, the Internet has become an integral part of modern societies, propelling the end user to the forefront of communication. All kinds of information is available, in all different formats and of varying topics and point of views.

The difficulty with this ever-growing multitude of resources is effectively surfing through the vast amount of information available on the Internet. How much of that information is factual, or even genuine? The real concern is not just with the dissemination of inaccurate or misleading information, but above all with malicious content. Fraud, theft and forgery exist online just as they do offline. If users are to benefit from the full advantages of the Internet, then confidence in the infrastructure is primary and of utmost importance.

Cyber threats such as malware and attacks are becoming extremely sophisticated. This is especially true with the increased presence of organized criminal groups online. The Internet has ceased to be the domain of the technically competent. User-friendly software and interfaces have enabled all types of users, including children and novices, to interact remotely. This new territory contains a gold-mine of valuable information and potential victims. The complicated infrastructure of the Internet also makes it more difficult to track down criminals.

But criminals are not the only threats to the Internet. The vulnerabilities of ICTs are a lure to terrorism and espionage. Cyber warfare and espionage have also made their appearance and can pose serious threats to critical information infrastructure.

Even though national measures are being taken, cyber threats remain an international problem. Loopholes in legal frameworks are being exploited by perpetrators and harmonization between existing laws is far from satisfactory. Coupled with the absence of appropriate organizational structures, there is a genuine problem in responding to cyber threats.

This is without counting the constant evolution and sophistication of such threats and the vulnerabilities in software, and more recently hardware, applications. With the phenomenal growth in mobile ICTs and new trends such as cloud computing and virtualization, it is increasingly likely that cyber threats will spread to new levels.

ITU: a unique global forum to discuss cybersecurity

ITU recognizes that information and technology security are critical priorities for the international community. Cybersecurity generally is in everyone's best interest and this can only be achieved through a collaborative effort. Cyber threat issues are global and therefore the solutions must be global too. It is vital that all countries arrive at a common understanding regarding cybersecurity, namely providing protection against unauthorized access, manipulation and destruction of critical

"ITU's commitment to building trust and security in ICTs remains as strong as ever. WSIS implementation, and notably Action Line C5, continue to be priorities in the ongoing work of the ITU. As technologies rapidly evolve and security concerns constantly change, the multistakeholder approach of the ITU has enabled it to keep pace with emerging issues. The Global Cybersecurity Agenda has promoted further cooperation and allowed for an even wider reach, enabling a truly international approach to cybersecurity challenges."

Mr. Houlin Zhao
ITU Deputy Secretary-General
& Chair of WSIS Task Force

resources. The ITU believes the strategy for a solution must identify those existing national and regional initiatives, in order to work effectively with all relevant players and to identify priorities.

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 least developed countries, developing and emerging economies, as well as developed countries. ITU is therefore an excellent forum for action and response to promote cybersecurity and to tackle cybercrime.

ITU and WSIS Implementation

The ITU, due to its long history, mandate and commitment, works hard to address cybersecurity challenges as these emerge and evolve. The ITU is promoting cybersecurity through a range of activities related to standardization and technical assistance to developing countries tailored to their specific needs. The ITU is made up of three Sectors: the Radiocommunication Sector (ITU-R), the Standardization Sector (ITU-T) and the Telecommunication Development Sector (ITU-D). At the World Summit on the Information Society (WSIS), world leaders and governments entrusted the ITU to take the lead in coordinating international efforts in the field of cybersecurity, as the sole Facilitator of Action Line C5, "Building confidence and security in the use of ICTs". 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.

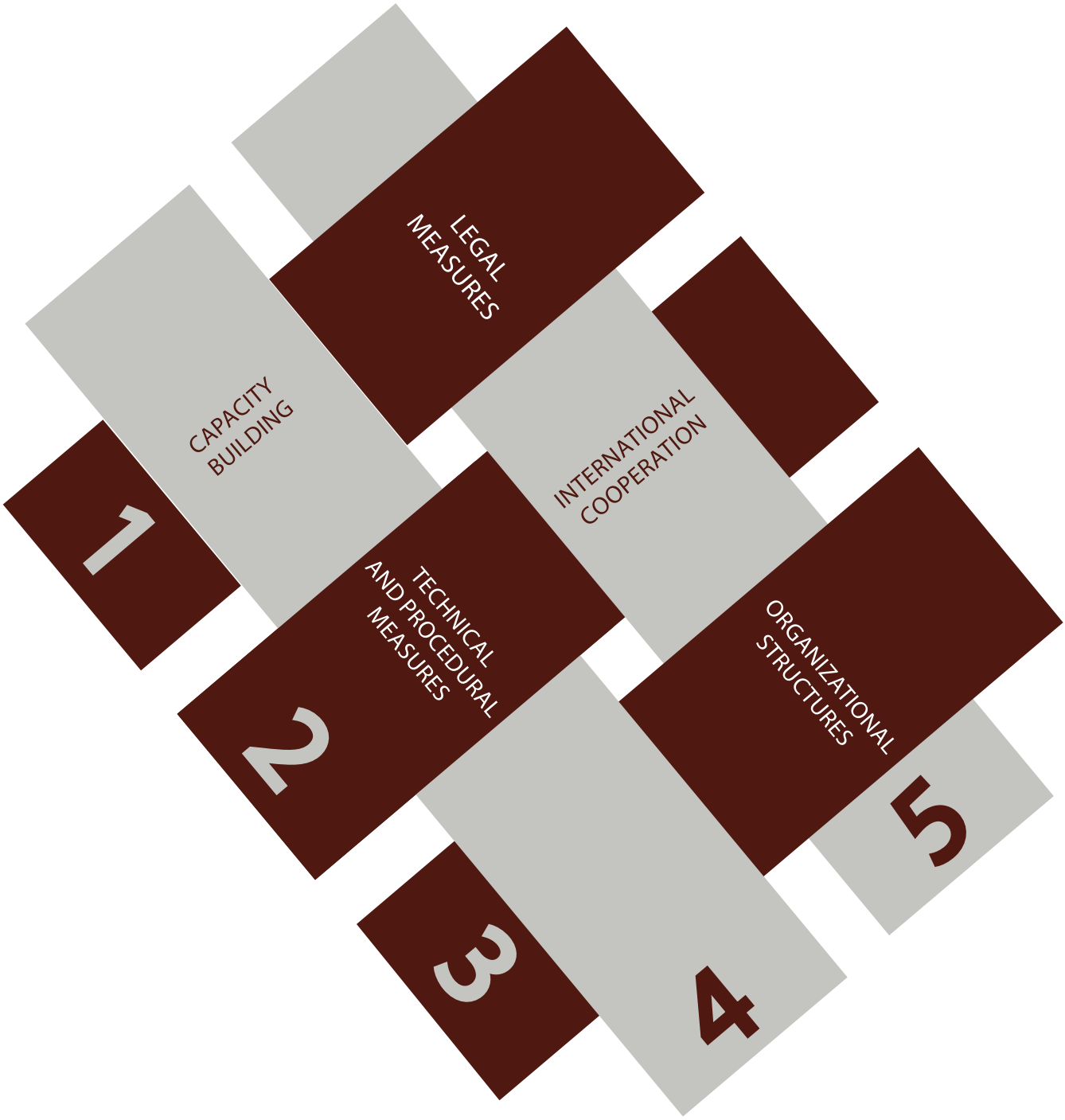
An International Framework for Cybersecurity: ITU's Global Cybersecurity Agenda

The Secretary-General's vision is a global information society in which trust and security in the use of ICTs is the norm for the benefit of mankind. For this reason, on 17 May 2007, the ITU launched the Global Cybersecurity Agenda (GCA) to provide a framework within which an international response to the growing challenges to cybersecurity can be coordinated and addressed. The GCA is based on international cooperation and strives to engage all relevant stakeholders in a concerted effort to build confidence and security in the information society. 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

Cyber criminals are an ever present menace in every country connected to the Internet. Organized crime has been on the rise because the Internet has proved a low risk, lucrative business arena. This is due to the fact that loopholes in national and regional legislation still remain, making it difficult to effectively track down criminals. The main problem is the lack of international harmonization regarding cybercrime legislation. Investigation and prosecution are difficult if the categorization of crimes differs from country to country. Some efforts to address this challenge have been undertaken, and although very valuable, they are still insufficient. The Internet is an international communication tool and, consequently, any solution to secure it must be sought at the global level.

ITU Cybercrime Legislation Resources

With its cybercrime legislation resources and material, the ITU is working to assist countries in understanding the legal aspects of cybersecurity in order to move towards harmonizing legal frameworks. Through these cybercrime legislation resources, ITU is addressing the first of the seven strategic goals of the GCA, which calls for the elaboration of strategies for the development of cybercrime legislation that is globally applicable and interoperable with existing national and regional legislative measures. 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 adoption by all countries of appropriate legislation against the misuse of ICTs for criminal or other purposes, including activities intended to affect the integrity of national critical information infrastructures, is central to achieving global cybersecurity. Since threats can originate anywhere around the globe, the challenges are inherently international in scope and require international cooperation, investigative assistance, and common substantive and procedural provisions. Thus, it is important that countries harmonize their legal frameworks to combat cybercrime and facilitate international cooperation. 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"[4] aims to help developing countries better understand the national and international implications of growing cyber-threats, assess the requirements of existing national regional and

4 The ITU publication Understanding Cybercrime: A Guide for Developing Countries, 2009, is available at: http://www.itu.int/ITU-D/cyb/cybersecurity/legislation.html

international instruments, and assist countries in establishing a sound legal foundation.

The Guide provides a comprehensive overview of the most relevant topics linked to the legal aspects of cybercrime. In its approach, the Guide focuses on the demands of developing countries. Due to the transnational dimension of cybercrime, the legal instruments are the same for developing and developed countries. However, the references used were selected for the benefit of developing countries. The Guide provides a broad selection of resources for a more in depth study of the different topics. Whenever possible, publicly available sources were used, including many free-of-charge editions of online law journals.

The Guide contains six main chapters. After an Introduction (Chapter 1), the Guide provides an overview of the phenomena of cybercrime (Chapter 2). This includes descriptions of how crimes are committed and explanations of the most widespread cybercrime offences such as hacking, identity theft and denial-of-service attacks. The Guide also provides an overview of the challenges as they relate to the investigation and prosecution of cybercrime (Chapters 3 and 4). After a summary of some of the activities undertaken by international and regional organizations in the fight against cybercrime (Chapter 5), the Guide continues with an analysis of different legal approaches with regard to substantive criminal law, procedural law, international cooperation and the responsibility of Internet Service Providers (Chapter 6), including examples of international approaches as well as good-practice examples from national solutions.

ITU Toolkit for Cybercrime Legislation[5]

The ITU Toolkit for Cybercrime Legislation aims to provide countries with sample legislative language and reference material that can assist in the establishment of harmonized cybercrime laws and procedural rules. The Toolkit is a practical instrument that countries can use for the elaboration of a cybersecurity legal framework and related laws.

The Sample Language provided in the Toolkit, while not a model law, was developed after a comprehensive analysis of the most relevant regional and international legal frameworks currently present. The Toolkit language is consistent with these laws and is intended to serve as a guide for countries desiring to develop, draft, or modify their own cybercrime laws. The Toolkit is intended to advance the global harmonization of cybercrime laws by serving as a central resource to help legislators, attorneys, government officials, policy experts, and industry representatives around the globe move their countries toward a consistent legal framework that protects against the misuse of ICTs.

The Toolkit's Sample Language may be customized to suit the laws of a particular country. Countries that model their cybercrime laws after the Toolkit's Sample Language will help advance a harmonized global framework, facilitate international cooperation, resolve jurisdictional and evidentiary issues, and deter cyber criminal behavior.

---

5 The ITU Toolkit for Cybercrime Legislation, 2009, is available at: http://www.itu.int/ITU-D/cyb/cybersecurity/legislation.html

In addition to the sample language, the Toolkit contains three additional sections of information that serve as practical aids in developing cybercrime legislation: (1) Explanatory Comments regarding certain provisions or aspects of the Sample Language, (2) a Matrix of International Cybercrime Laws that compares the provisions of various countries' laws, and (3) a listing of useful reference materials of various works, laws, books, and articles that discuss cybercrime laws and issues.

The development of the ITU Toolkit for Cybercrime Legislation was undertaken by a multidisciplinary international group of experts.

TECHNICAL AND PROCEDURAL MEASURES

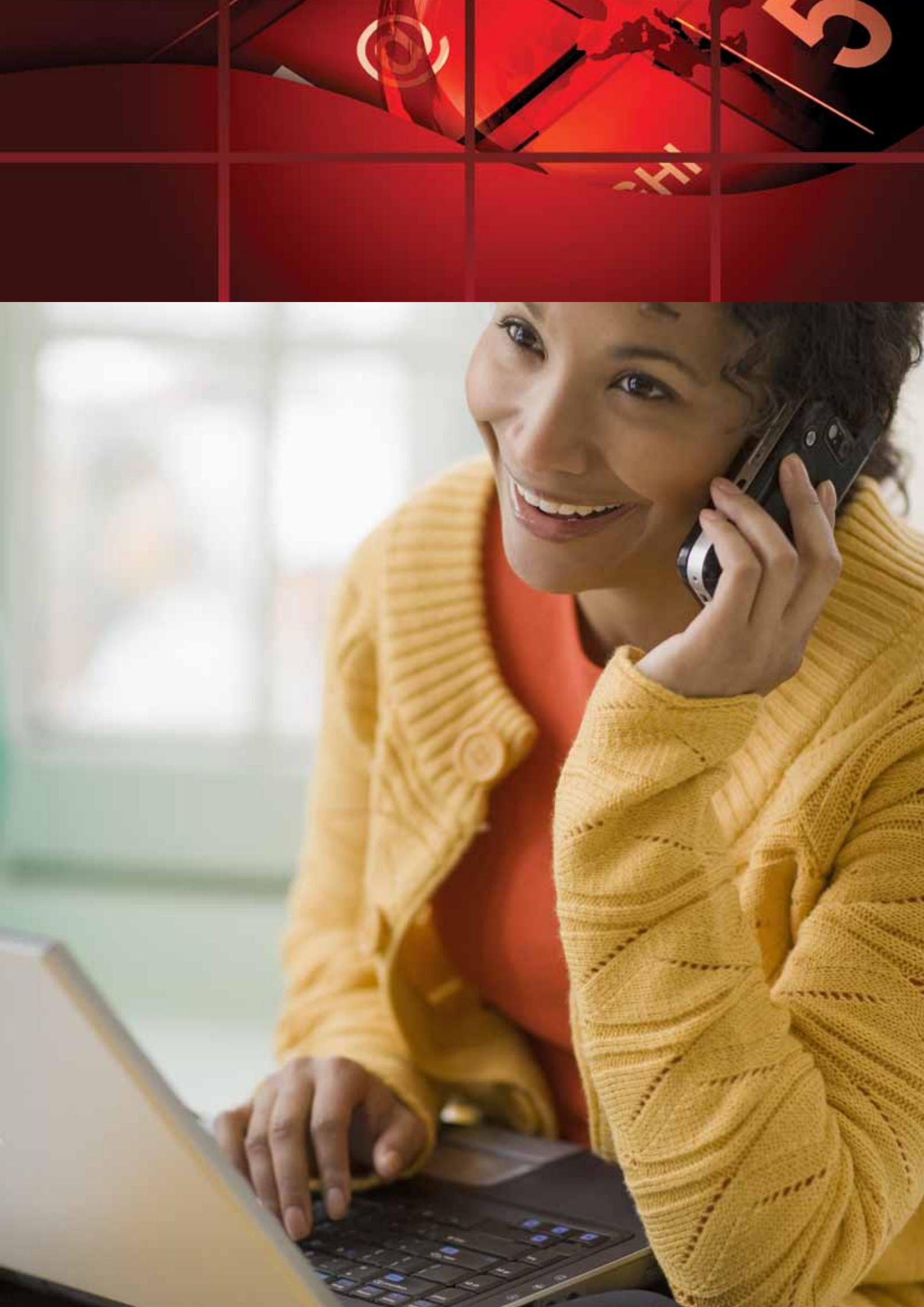
ICTs are a vital tool in information societies. However, they continue to be exploited by malevolent users and this phenomenon is becoming intrinsically linked to organized crime on the Internet. Vulnerabilities in software applications are purposely sought out in order to create malware that will enable unauthorized access and modification, thus compromising integrity, authenticity and confidentiality of the ICT networks and systems. With the increasing sophistication of malware, these threats cannot be overestimated and they could have dire consequences if critical information infrastructures are affected.

ITU Standardization Work

ITU's Standardization Sector (ITU-T) holds a unique position in the field of standardization: its work brings together the private sector and governments to coordinate work and promote the harmonization of security policy and security standards on an international scale.

Standards development bodies have a vital role to play in addressing security vulnerabilities in protocols. As well as many key security Recommendations, ITU has developed overview security requirements, security guidelines for protocol authors, security specifications for IP-based systems it defines (NGN, H.323, IPCableCom, etc), guidance on how to identify cyber threats and countermeasures to mitigate risks. ITU also provides the international platform for the development of the protocols that protect current and Next-Generation Networks (NGN). ITU's work addresses security aspects in NGN architecture, quality of service, network management, mobility, billing and payment for NGN. ITU's work on secure communication services reviews enhancements to security specifications for mobile end-to-end data communications and considers security requirements for web services and application protocols.

In the move to Internet Protocol (IP)-based services, ITU's H.235.x series Recommendations on "H.323 Security" defines the security infrastructure and services (including authentication and privacy) for use by the H.300-Series IP multimedia systems



(such as VoIP and videoconferencing) in point-to-point and multipoint applications. The H.235.x standards provide privacy to service providers and enterprises, whilst ensuring interoperability of multimedia products. The identity of users communicating through IP media is correctly authenticated and authorized using the H.235.x Recommendation, protecting their communications against different critical security threats.

Real-time multimedia encryption adds a further layer of security, guarding against call interception. ITU's J.170 "IPCablecom Security Specification" defines security requirements for IPCablecom architecture enabling cable TV operators to deliver secure two-way capability in the provision of a variety of IP services, including VoIP.

ITU's work on security covers a broad range of activities in security from network attacks, theft or denial of service, theft of identity, eavesdropping, telebiometrics for authentication, security for emergency telecommunications and telecommunication network security requirements. ITU's X.805 Recommendation defines the security architecture for systems providing end-to-end communications that can provide end-to-end network security. This Recommendation allows operators to pinpoint vulnerable points in a network and address them. ITU's security framework extends this with guidelines on protection against cyber attacks.

The results of ITU's work are evident: one of the most important security standards in use today is X.509, an ITU-developed Recommendation for electronic authentication over public networks. X.509 is the definitive reference for public-key certificates and designing applications related to public key infrastructure (PKI). The elements defined within X.509 are widely used in securing connections between web-browsers and servers to agreeing the encryption key that protects the information exchanged and providing the digital signatures that enable e-commerce transactions. Public key certificates are also used to authenticate and protect e-mail – an electronic document with a digital certificate supported by an X.509 certificate is widely recognized as the most credible form of electronic document. ITU's work on electronic authentication has helped enable jurisdictions around the world to recognize e-mail as legal documents and to accord legal status to electronic signatures.

Recently, ITU-T X.1205 "Overview of Cybersecurity" was approved. It provides a definition of cybersecurity and a taxonomy of security threats. It discusses the nature of the cybersecurity environment and risks, possible network protection strategies, secure communications techniques and network survivability (even under attack).

Currently, all ITU Study Groups conduct security-related activities and review security questions as part of their work, while the Telecommunication Standardization sector's Study Group 17 acts as the overall lead study group on telecommunication security and identity management. In 2002, ITU agreed to cooperate with other standards development organizations in setting standards for security, monitoring security work carried out around the world and considering best practices and effective solutions. ITU hosts a regular joint security workshop inviting non-member attendees to contribute to a roadmap for future work and coordination between other standards development organizations.


Customer : Hello
Advisor: Good afternoon how can I help ...
Customer: I have a problem with .....
Customer Details
Gender: Female
Name: Mrs Smith
Operating System: Yes
Current Customer: Yes

ITU-T Study Group 17

Study Group 17 is the lead study group on telecommunications security and identity management. It is responsible for studies relating to security, including cybersecurity, countering spam and identity management and handles security guidance and the coordination of security related work across all ITU-T study groups. Its role as the lead study group on work related to security was confirmed by the ITU-T World Telecommunication Standardization Assemblies (WTSA) in 2000, 2004 and 2008, in close collaboration with ISO/IEC, as a tripartite joint action. WTSA-08 added to Study Group 17 the lead study group role for identity management. Study Group 17 has approved over one hundred Recommendations on security for communications, mainly in the X series of Recommendations, either by itself, or jointly with ISO/IEC or other relevant organizations. It regularly updates the manual on "Security in telecommunications and information technology" as an overview of security issues and the deployment of ITU-T Recommendations for secure telecommunications across all ITU-T Study Groups (the third manual was issued in August 2006, the fourth edition is scheduled for publication later in 2009).

Study Group 17 also electronically publishes a Security Compendium on its website containing a catalogue of approved ITU-T Recommendations related to security and presenting an extract of security definitions from ITU-T and other sources. The role of Study Group 17 was confirmed and reinforced by various Resolutions adopted at the WTSA-08 in Johannesburg:

- Resolution 50 on "Cybersecurity" guiding ITU-T work to build Recommendations sufficiently robust to prevent exploitation by malicious parties;
- Resolution 52 on "Countering and combating spam", seeking to integrate the technical means to combat spam into the work of ITU-T study groups and SG 17 Recommendations.

Study Group 17 is also working on the implementation of WTSA-08 Resolution 58 to "Encourage the creation of national Computer Incident Response Teams, particularly for developing countries".

ICT Security Standards Roadmap promoting collaboration between international standards bodies

The Roadmap was launched by ITU Study Group 17, and became a joint effort in January 2007, when the European Network and Information Security Agency (ENISA) and the Network and Information Security Steering Group (NISSG) joined the initiative. The ICT Security Standards Roadmap promotes the development of security standards by highlighting existing standards, current work and future standards among key standards development organizations. The Roadmap informs users about security standards. It contains five parts:

“ITU has developed many important security standards and guidelines for best practices like X.509 and X.805. We will continue this effort based on past success with the commitment from our membership - dedicated individuals from governments, the private sector and civil society.”

Mr. Malcolm Johnson
Director, ITU Telecommunication Standardization Bureau (TSB)

Part 1: ICT Standards Development Organizations and Their Work outlines the structure of the Roadmap and describes the different standards organizations, their structure and the work they are undertaking in security standards (including ITU, ISO, IEC, IETF, OAIS, ATIS, ETSI, IEEE, 3GPP and 3GPP2), complete with links to existing glossaries of security.

Part 2: Approved ICT Security Standards provides a database summarizing the catalogue of approved standards. It contains guidance on how to use the database, a taxonomy, as well as a list of acronyms and abbreviations.

Part 3: Security standards under development summarizes standards under development by ITU and ISO/IEC (rather than existing standards). It will also describe the inter-relationships between the work of standardization bodies. This catalogue is also being developed as a database.

Part 4: Future needs and proposed new security standards outlines future areas of work in security standards, where gaps have been identified or proposals made for new standards work.

Part 5: Best practices was added to the Roadmap in May 2007, as a repository of security related best practices contributed by members and stakeholders. The Roadmap will include the work of other standards organizations in future editions. It is being transformed into a database format.

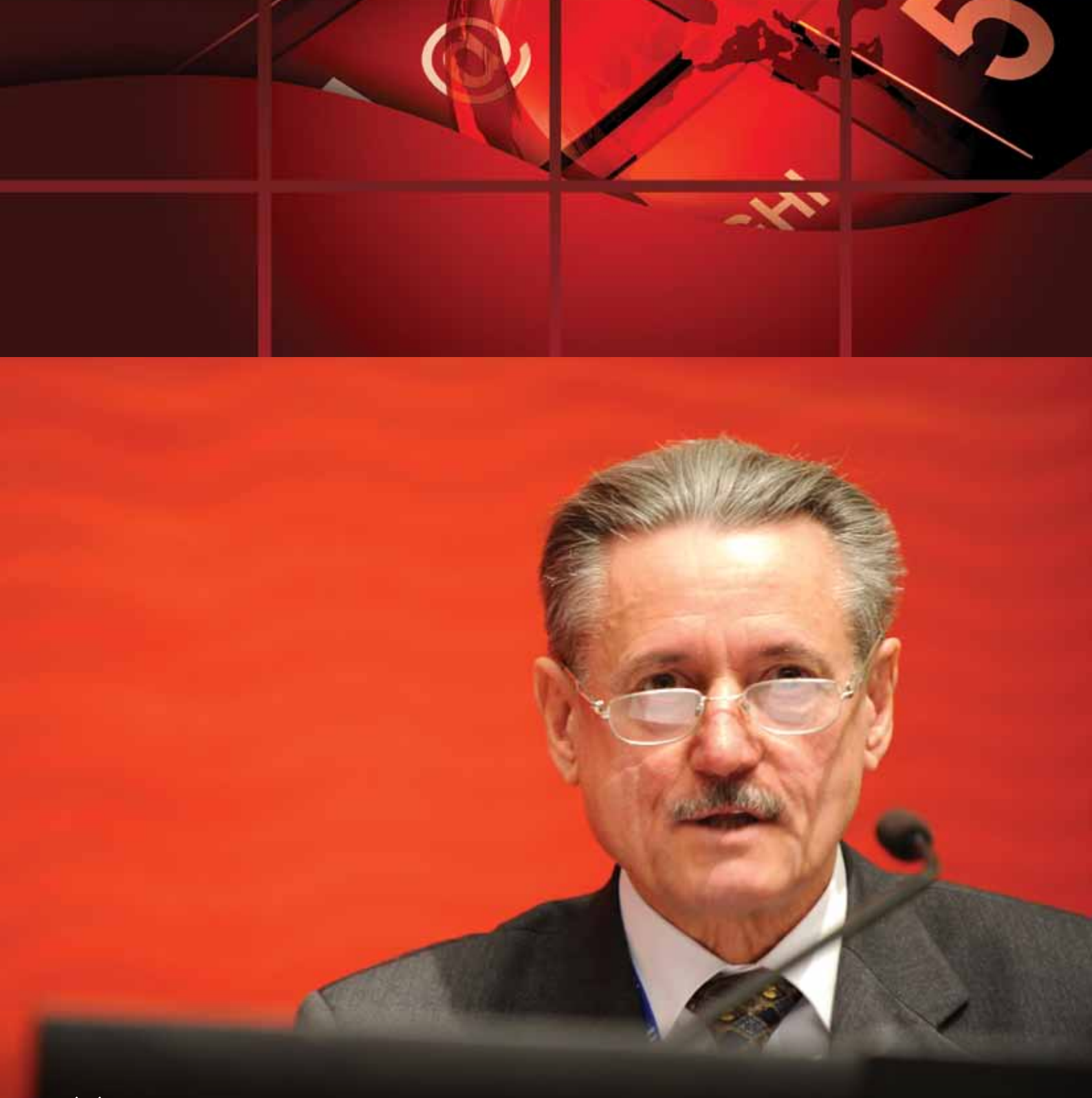
ITU Radiocommunications

Radio spectrum global frequency management is increasingly important for building confidence, security and creating an enabling environment in the use of ICTs. Wireless applications, such as 3G, are becoming an integral part of daily life, and the global use and management of frequencies require a high level of international cooperation.

ITU's Radiocommunication Sector (ITU-R) mission is to ensure rational, equitable, efficient and economical use of the radio-frequency spectrum by all radiocommunication services, including those using satellite orbits, and to carry out studies and adopt Recommendations on radiocommunication matters. It plays a pivotal role in facilitating complex intergovernmental negotiations needed to develop legal binding agreements between sovereign states in an increasingly 'unwired' world.

International radiocommunication provisions are embodied in the ITU Radio Regulations (*treaty status*) that incorporates the decisions of the World Radiocommunication Conferences (WRC's) and in world and regional plans adopted for different space and terrestrial services. ITU Radio Regulations agreements apply to frequencies ranging from 9 kHz to 400 GHz and include information on how radio frequency is shared around the globe.

WRCs are held every 3 to 4 years to update the international treaty governing the use of the radio-frequency spectrum (where some 40 different radio services compete for allocations



“Cybersecurity remains an important component of ITU-R’s activities with the establishment of fundamental security principles for IMT-2000 (3G) networks, network management architecture for digital satellite systems and performance enhancements of transmission control protocol over satellite networks. ITU-R’s work in radio spectrum global frequency management and its latest Recommendations on generic requirements and the protection of radiocommunications has been vital in building confidence and security and creating an enabling environment in the use of ICTs.”

Mr. Valery Timofeev
Director, ITU Radiocommunication Bureau (BR)

for spectrum) and the geostationary satellite and non-geostationary satellite orbits.

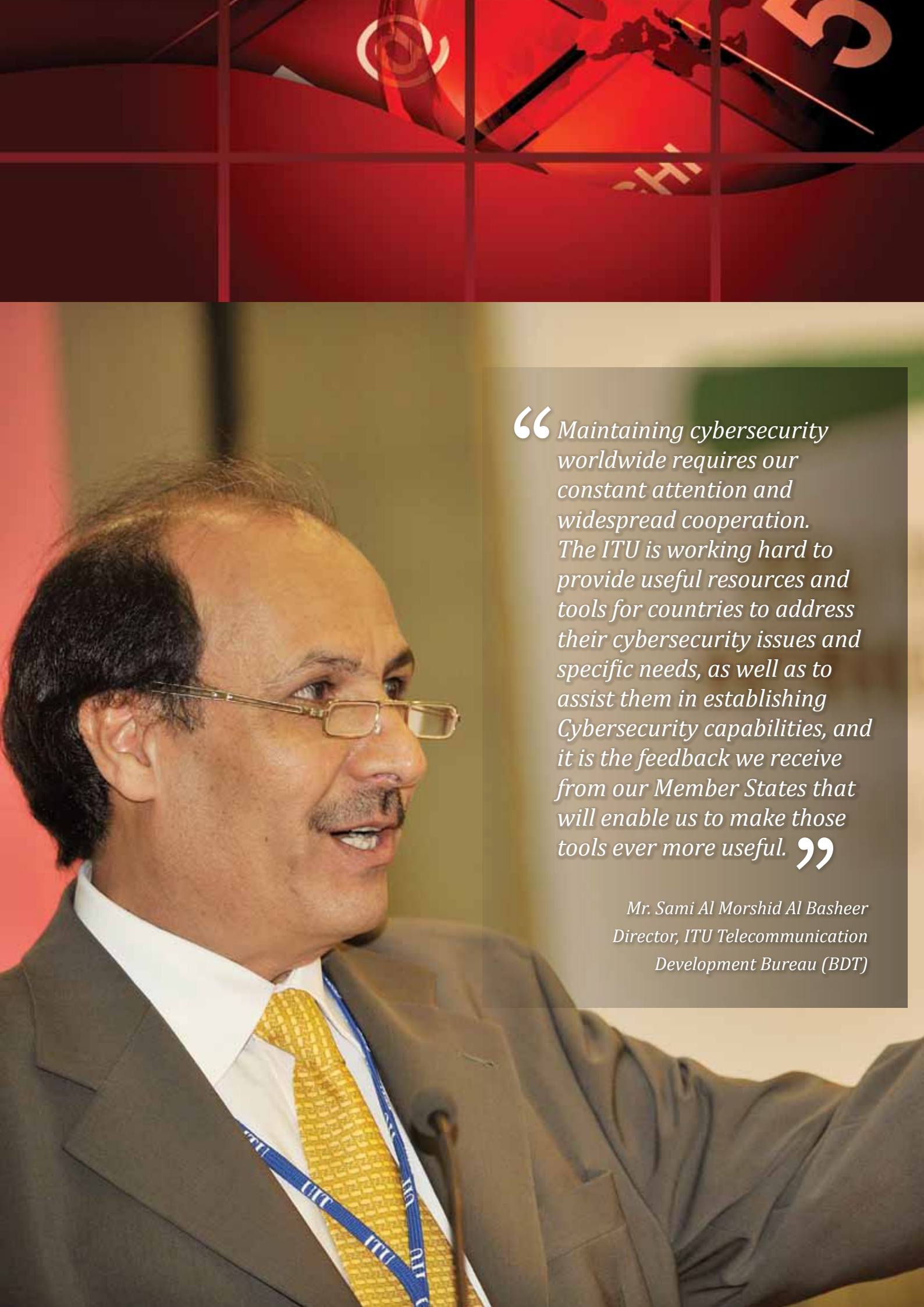
ITU-R specializes in developing radio standards, including spectrum identification and harmonization applicable to national, regional and international broadband network infrastructure including the capacity to countries and their citizens for new ICT-based services through satellite systems. ITU-R ensures interference-free operation of radiocommunication systems and facilitates any new developments and the continuation of satellite services in a safe way.

Safeguarding quality of service against degradation or denial of service is vital for the secure functioning of networks in data transmission and service provision and many of the Radiocommunication Sector (ITU-R)'s latest Recommendations on generic requirements and the protection of radiocommunications against interference are relevant for security.

ITU's work in radiocommunication standardization continues, matching the constant evolution in modern telecommunication networks. ITU established clear security principles for IMT-2000 (3G) networks (Recommendation ITU-R M.1078 and Recommendations M.1223, M.1457, M.1645 are also relevant). ITU recommended early on that the security provided by mobile broadband IMT-2000 (3G) networks should be comparable to contemporary fixed networks. ITU has also issued recommendations on security issues in network management architecture for digital satellite systems (Recommendation ITU-R S.1250) and performance enhancements of transmission control protocol over satellite networks (Recommendation ITU-R S.1711).

IMPACT Global Response Centre

As part of the ITU's collaboration with the International Multilateral Partnership Against Cyber Threats (IMPACT), the Global Response Centre (GRC) plays a pivotal role in realizing the GCA objective of putting technical measures in place to combat new and evolving cyber-threats. The two prime highlights of the GRC are NEWS (*Network Early Warning System*) and ESCAPE (*Electronically Secure Collaboration Application Platform for Experts*). The GRC is designed to be the foremost cyber threat resource centre in the world. Working with leading partners including academia and governments, the Centre will provide the global community with a real-time aggregated early warning system. NEWS will help countries identify cyber threats early on and provide critical guidance on what measures to take to mitigate them. The GRC will also provide ITU Member States with access to specialized tools and systems, including the recently-developed ESCAPE platform. ESCAPE is an electronic tool that enables authorized cyber-experts across different countries to pool resources and collaborate with each other remotely, yet within a secure and trusted environment. By pooling resources and expertise from many different countries on short notice, ESCAPE will enable individual nations and the global community to respond immediately to cyber-threats, especially during crisis situations.



"Maintaining cybersecurity worldwide requires our constant attention and widespread cooperation. The ITU is working hard to provide useful resources and tools for countries to address their cybersecurity issues and specific needs, as well as to assist them in establishing Cybersecurity capabilities, and it is the feedback we receive from our Member States that will enable us to make those tools ever more useful."

Mr. Sami Al Morshid Al Basheer
Director, ITU Telecommunication Development Bureau (BDT)

ORGANIZATIONAL STRUCTURES

Watch and warning systems and incident response are essential when it comes to responding to cyber attacks, as is the free flow of information, collaboration and cooperation within and between national organizational structures. Individuals, organizations and governments are increasingly dependent on globally interconnected networks. In order to protect network infrastructures and address threats, coordinated national action is required to prevent, respond to and recover from incidents. Collaboration at all levels of government and with the private sector, academia, regional and international organizations, is necessary to raise awareness of potential attacks and take steps towards remediation. Effective incident management also requires consideration of funding, human resources, training, technological capability, government and private sector relationships, and legal requirements. Efforts are being made to bring together organizational structures at the national and regional level in order to facilitate communication, information exchange and the recognition of digital credentials across different jurisdictions. However, more needs to be done at the global level and international cooperation between these different structures is indispensable.

In this regard, ITU is working with Member States to identify the specific cybersecurity needs that they have and, based on this work, with the relevant national, regional and international organizations to implement these activities. Regional Cybersecurity Forums organized by the ITU Development Sector together with regional and national stakeholders serve as a good first step for countries to get involved in ITU's cybersecurity capacity building activities.

Several regional initiatives are already recommending that Member States establish national cybersecurity response centers, such as computer incident response teams (CIRTs), noting that there is still a low level of computer emergency preparedness within many countries, particularly developing countries and that a high level of interconnectivity of ICT networks could be affected by the launch of an attack from networks of the less-prepared nations. ITU WTSA-08 Resolution 58[6] further emphasizes this and encourages ITU Member States to move forward on creating national CIRTs. Given the importance of having an appropriate level of computer emergency

6 *ITU WTSA Resolution 58: Encourage the creation of national computer incident response teams, particularly for developing countries (Johannesburg, 2008), available at: http://www.itu.int/dms_pub/itu-t/opb/res/T-RES-T.58-2008-PDF-E.pdf*

preparedness in all countries and the need to establish national computer incident response teams and ensure coordination within and among the different regions, countries in need of assistance in this area are encouraged to contact the ITU, specifying existing cybersecurity preparedness and detailing their national requirements in this area. In implementing these and other activities with Member States, ITU is working with partners from both the public and private sectors in innovative and collaborative partnerships.

IMPACT Security Assurance Division

In partnership with leading ICT experts, IMPACT aggregates and develops global best practice guidelines, creating an international benchmark that is especially relevant for governments. This division conducts, upon request, independent ICT security audits on government agencies or critical infrastructure companies, thereby ensuring that these organizations subscribe to the highest security standards. The Security Assurance Division functions as an independent, internationally-recognized, voluntary certification body for cybersecurity.

CAPACITY BUILDING

Capacity building needs to be promoted in order to develop a sustainable and proactive culture of cybersecurity. People are the weakest link. One of the key challenges of cybersecurity is effectively educating the end user. Understanding and awareness of the potential dangers are critical if the end-user is to benefit from ICTs safely. This is a matter that concerns all stakeholders from governments and industry to education both at school and at home. 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 cyber environment and of the threats inherent to cyber space are vital. Programmes aimed at creating a level playing-field in raising basic awareness and building capacity at all levels are important, and these also need to be undertaken within the international arena.

Within the framework of GCA and in line with ITU mandate to assist Member States in developing cybersecurity capacity, the ITU works to facilitate the implementation and deployment of cybersecurity capabilities necessary to combat cyber-threats. As such, the ITU is playing a key role in implementing the main goals of GCA while responding to the needs of Member States.

ITU National Cybersecurity/CIIP Self-Assessment Tool

The ITU National Cybersecurity/CIIP Self-Assessment Tool[7] is a practical initiative to assist ITU Member States who wish to design their national approach for cybersecurity and critical information infrastructure protection (CIIP). The Tool is one of a number of complementary cybersecurity resources that ITU is currently developing as part of a comprehensive cybersecurity toolkit for ITU Member States.

Cybersecurity and CIIP are the shared responsibilities of government, business, other organizations, and individual users who develop, own, provide, manage, service and use information systems and networks (the "participants"[8]).

---

7 Information about the ITU National Cybersecurity Self-Assessment Tool is available at: http://www.itu.int/ITU-D/cyb/cybersecurity/projects/readiness.html

8 "Participants" as defined in UN Resolution 57/239: Creation of a Global Culture of Cybersecurity, 2002, available at http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_57_239.pdf ; UN Resolution 58/199: Creation of a global culture of cybersecurity and the protection of critical information infrastructures, 2004, available at http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_58_199.pdf .

Managing inherent security risks requires the active cooperation of all participants, addressing the security concerns relevant to their roles. The collective goal is to prevent, prepare for, respond to, and recover from any incidents rapidly, while minimizing damage. In any interconnected system, roles and responsibilities often overlap. Only when all participants share a common understanding of the security objectives, how to achieve them and of their individual roles in the effort, can this collective goal of a safe and secure communications be achieved.

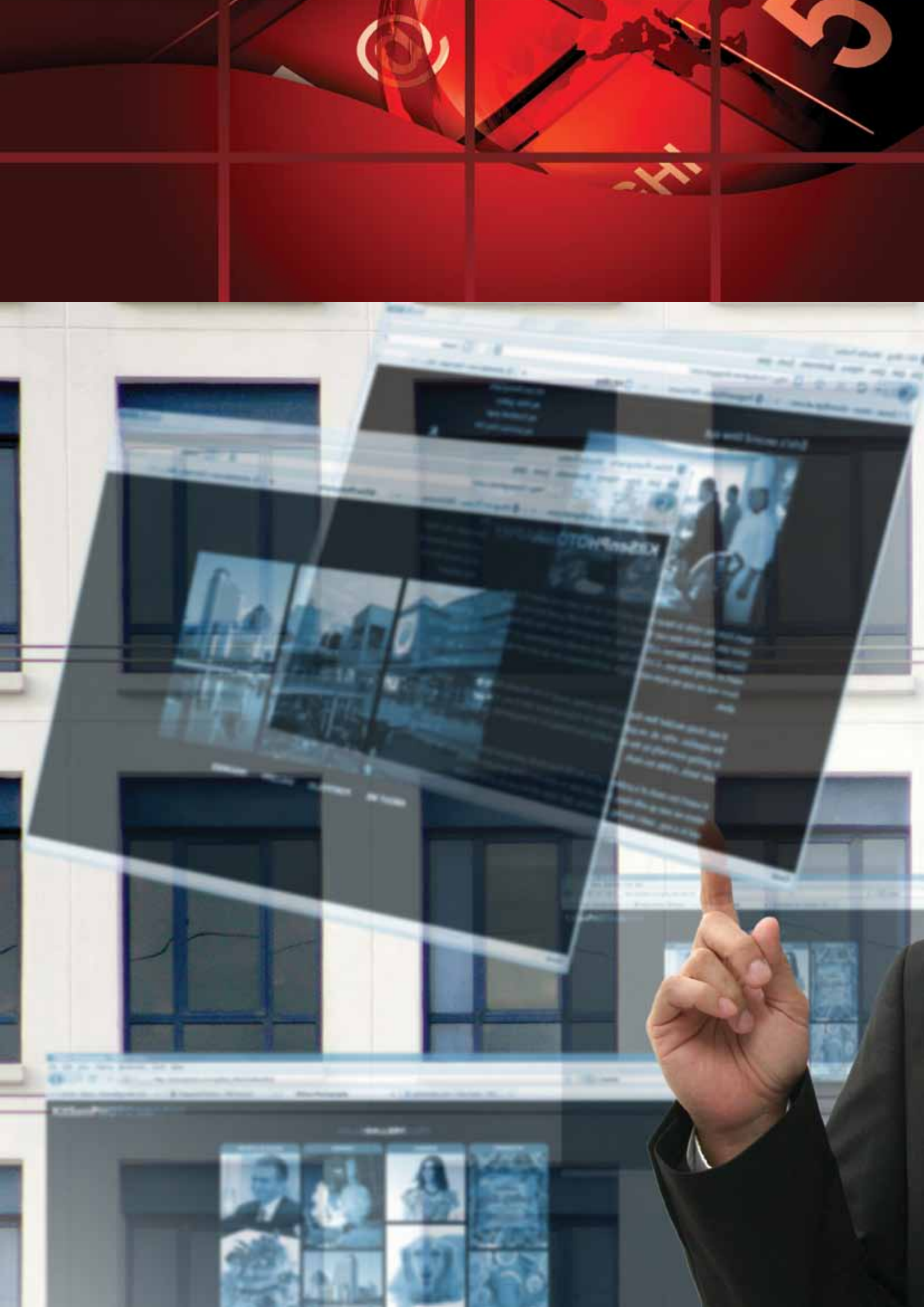
Governments are in a position to lead national efforts to enhance cybersecurity and improve CIIP. The preparation of a national cybersecurity strategy has proven to be a valuable tool for effective and coordinated action. By establishing a common vision and delineating roles and responsibilities, such a strategy can provide a guide for managing risks inherent in ICT use and addressing cybersecurity and CIIP. Such a strategy can also provide valuable support for enhanced regional and international cooperation. After a nation has gained valuable domestic experience of addressing cybersecurity and CIIP issues, it can participate more meaningfully and make a more valuable contribution to global cooperative security efforts.

In this regard, the **ITU National Cybersecurity/CIIP Self-Assessment Tool** aims to assist ITU Member States in developing their national strategy by examining their existing capacities for addressing challenges to cybersecurity and CIIP, identifying their requirements and outlining a national response plan. It is directed at leadership in the policy and management levels of government. The Tool also seeks to produce a snapshot of the current state of national cybersecurity and CIIP efforts, identify goals, and define the roles of the key participants in order to set priorities, establish timeframes and provide metrics.

The ITU, through its Telecommunication Development Sector, provides Member States with the assistance needed to undertake an initial self-assessment, as well as providing relevant support for countries which are in the process of developing and/or reassessing their national cybersecurity strategies.

ITU Toolkit for Promoting a Culture of Cybersecurity

The purpose of the ITU Toolkit for Promoting a Culture of Cybersecurity is to provide guidelines on how to raise awareness on cybersecurity issues for SMEs, consumers and end-users in developing countries. Considering that personal computers, mobile phones, and other devices are becoming ever more powerful, that technologies are converging, that the use of ICTs is becoming more and more widespread, and that connections across national borders are increasing, all participants who develop, own, provide, manage, service and maintain information networks must understand cybersecurity issues and take action appropriate to their roles to protect networks. Governments can, and should, take a leadership role in promoting a culture of cybersecurity and in supporting the cybersecurity and cyber safety efforts undertaken by other stakeholders.



ITU Botnet Mitigation Toolkit

ITU is working with experts on developing a practical Botnet Mitigation Toolkit[9] to assist developing countries in particular to deal with the growing problem of botnets. The Botnet Mitigation Toolkit is a multi-stakeholder, multi-pronged approach to track botnets and mitigate their impact, with a particular emphasis on the problems specific to emerging internet economies.

IMPACT Training and Skills Development Centre

In collaboration with leading ICT companies and institutions, IMPACT conducts high-level briefings for the benefit of representatives of ITU Member States. Many of IMPACT's key partners have made available their respective Chief Technical Officers, Chief Research Officers and other experts in a unique high-level IMPACT programme to keep governments abreast of present and future cyber threats. The ITU contributes its experience in capacity-building and developing frameworks for policy response to this programme. Such high-level, cross-industry briefings give ITU Member States invaluable exposure and privileged private sector insight about the latest trends, potential threats and emerging technologies.

IMPACT Research Division

The focus of the Research Division is to direct academic attention, including from universities and research institutes, to areas of concern that may not currently be adequately addressed. This includes research into new areas, as well as specialized niche areas. With a small user base, niche technologies may not be commercially viable for industry-oriented solutions, making governments or organizations using such technologies vulnerable to threats. IMPACT is committed to making facilities available and encouraging joint research efforts to address these specific areas of concern. In collaboration with the ITU, IMPACT is making its research network available for the benefit of interested ITU Member States. Besides the academic network, IMPACT global headquarters provides ITU membership with access to specialized ICT laboratories, specialized equipment, resource centre and other facilities.

9 *Information about the ITU Botnet Mitigation Toolkit is available at: http://www.itu.int/ITU-D/cyb/cybersecurity/projects/botnet.html*

INTERNATIONAL COOPERATION

The Internet and ICTs have enabled interconnection between countries that was not possible before. Countries cannot easily close their borders to incoming cyber threats and cannot either contain those coming from within. Attempts to solve these challenges at national or regional levels are important, but they are undermined. Cybersecurity is as global and far-reaching as the Internet. Therefore solutions need to be harmonized across all borders. This necessarily entails international cooperation, not only at government level, but also with industry, non-governmental and international organizations. Cybersecurity concerns all types of measures. For this reason, the GCA seeks to harness the power of multi-stakeholder collaboration in order to arrive at global strategies to enhance cybersecurity.

UN Delivering as One on Cybersecurity and Cyberpeace

In line with the spirit of UN Delivering as One on Cybersecurity and Cyberpeace, ITU has coordinated its efforts, to promote cybersecurity, to combat cybercrime and to address cyber-threats, with UNODC, UNIDIR, UNICEF and UNICRI inter alia, in the following areas:

Combating Cybercrime: ITU and UNODC are working together on identity-related crime and identity management related issues.

Building Capacity: ITU, UNIDIR and UNICRI are working together to build capacity and raise awareness including action oriented research of the challenges to cybersecurity and cyber-peace.

Child Online Protection: ITU, together with UNICEF, UNICRI, UNODC and other stakeholders, are working to promote child online safety.

High-Level Expert Group

The High-Level Experts Group (HLEG) initiated the GCA process by giving advice on strategies in all five work areas. The HLEG comprised 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 responsibilities of the HLEG were to meet and further develop the GCA, by proposing refinements to its main goals, analyze 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 and finally to provide guidance on possible long-term strategies and emerging trends in cybersecurity. The HLEG met on multiple occasions at the ITU and in November 2008, the ITU published their strategies in a Global Strategic Report. 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 the ITU Secretary General during Council 2008. Those proposals that were considered were reviewed by all the ITU Sectors, linked to the relevant ITU mandate and taken into account in the work programmes of the Sectors.

International Multilateral Partnership Against Cyber Threats

The International Multilateral Partnership Against Cyber Threats (IMPACT) is an international public-private initiative dedicated to enhancing the global community's capacity to prevent, defend and respond to cyber threats. In May 2008, the ITU was invited to become a member of the IMPACT Advisory Board. In November 2008, this collaboration came to fruition, with IMPACT's headquarters in Cyberjaya, Malaysia formally becoming the GCA's operational, physical, state-of-the-art home. The ITU maintains a 'virtual showcase' in Geneva of the early warning system, crisis management and real-time analysis of global cyber-threats. All IMPACT-based initiatives provide services in the five work areas of the GCA.

IMPACT Centre for Policy and International Cooperation

Under the ITU leadership, and together with partners such as United Nations agencies, Interpol, Council of Europe and OECD among others, the Centre for Policy & International Cooperation contributes to the formulation of new policies and the harmonization of national laws around a variety of issues relating to cyber threats, including cybercrimes. The Centre for Policy & International Cooperation also provides advisory services to interested ITU Member States on policy and regulatory matters for cybersecurity. With the support of the ITU, the Centre fosters international cooperation through specific programs such as coordinated cyber-drill exercises between countries.

ITU Cybersecurity Gateway

The purpose of the **ITU Cybersecurity Gateway**[10] 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 cybercrime related area. The Cybersecurity Gateway can serve as a platform to make stakeholders more aware of the various actors and groups working on the different areas of cybersecurity at the national, regional and

10 The ITU Cybersecurity Gateway can be found at: http://www.itu.int/cybersecurity/gateway/

international level. 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.

Child Online Protection

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. The key objectives of the initiative are to:

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

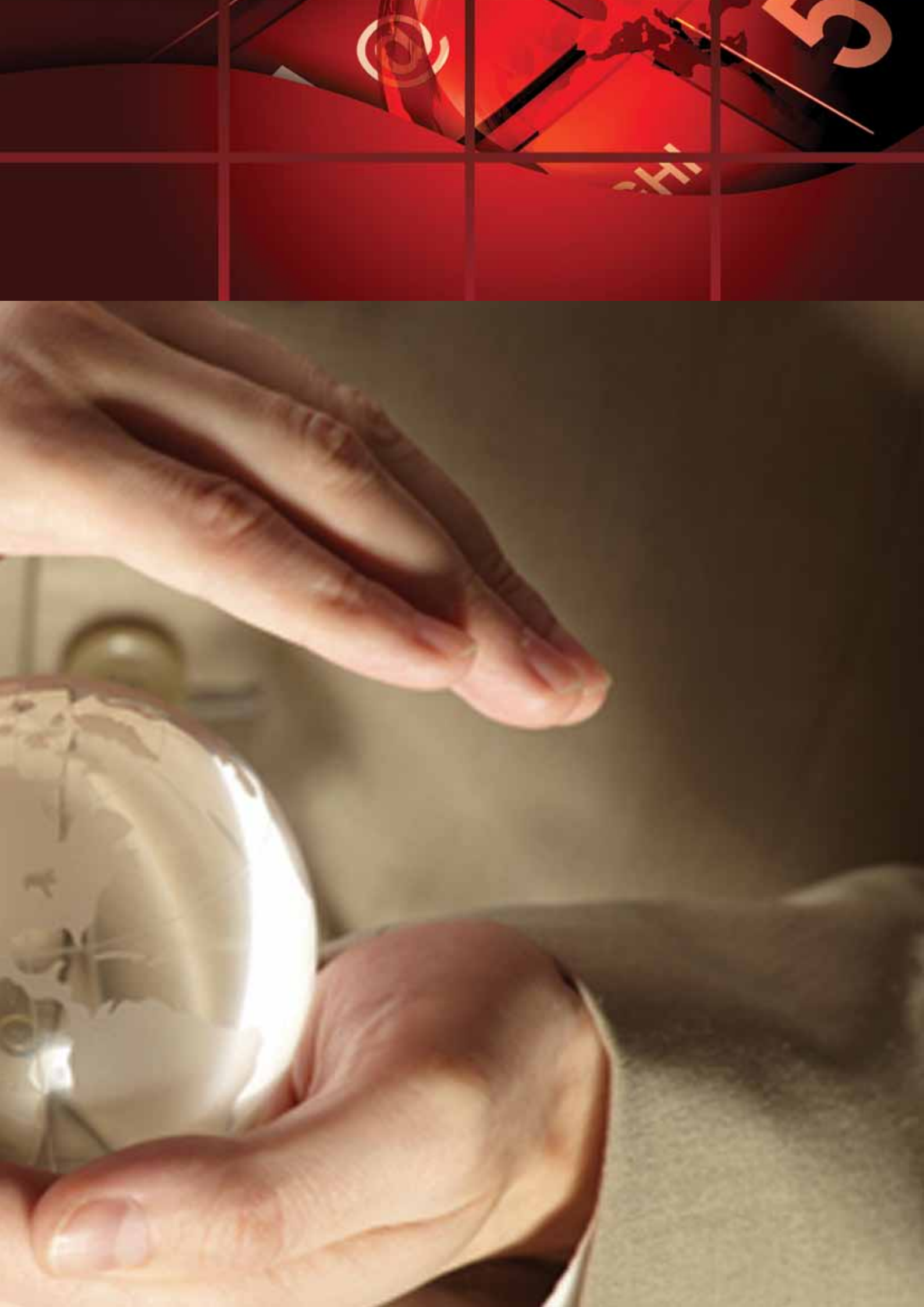
The COP initiative draws together an effective package of policies and practices, education and training, infrastructure and technology, and awareness and communication. The COP initiative is based on a multi-stakeholder approach and the belief that every organization - whether online or mobile, educator or legislator, technical expert or industry body - has something to contribute.

Conclusion

The ITU takes very seriously 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.

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 rings true also for cyber threats as they are intrinsically linked to ICT evolution.

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.



List of Acronyms

ATIS	Automatic Terminal Information Service
CIRT	Computer Incident Response Team
CIIP	Critical Information Infrastructure Protection
COP	Child Online Protection
DDOS	Distributed Denial of Service
ENISA	European Network and Information Agency
ETSI	European Telecommunications Standards Institute
GCA	Global Cybersecurity Agenda
ICTs	Information and Communication Technologies
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IMPACT	International Multilateral Partnership Against Cyber Threats
IMT-2000	International Mobile Telecommunications-2000
IP	Internet Protocol
ISO	International Organization for Standards
ITU	International Telecommunication Union
NGN	Next Generation Network
NISSG	Network and Information Security Steering Group
OAIS	Open Archival Information System
OECD	Organisation for Economic Cooperation and Development
PKI	Public Key Infrastructure
QoS	Quality of Service
UN	United Nations
WSIS	World Summit on the Information Society
WTSA	World Telecommunication Standardization Assembly

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 (Johannesburg, 2008)

"Cybersecurity"

Resolution 52 of the ITU World Telecommunication Standardization Assembly (Johannesburg, 2008)

"Countering and combating spam"

Resolution 58 of the ITU World Telecommunication Standardization Assembly (Johannesburg, 2008)

"Encourage the creation of national Computer Incident Response Teams, particularly for developing countries"

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 E.408

"Telecommunication networks security requirements"

ITU-T E.409

"Incident organization and security incident handling: Guidelines for telecommunication organizations"

ITU-T H.235 Series Recommendations on H.323 Security

ITU-T J.170

"IPCablecom security specification"

ITU-T 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 X.805

"Security architecture for systems providing end-to-end communications"

ITU-T X.811

"Information technology – Open Systems Interconnection – Security frameworks for open systems: Authentication framework"

ITU-T X.812

"Information technology – Open Systems Interconnection – Security frameworks for open systems: Access control framework"

ITU-T X.1031

"Security architecture aspects of end users and networks in telecommunications"

ITU-T X.1034

"Framework for extensible authentication protocol (EAP)-based authentication and key management"

ITU-T X.1035

"Password-authenticated key exchange (PAK) protocol"

ITU-T X.1036

"Framework for creation, storage, distribution and enforcement of policies for network security"

ITU-T X.1051

"Information technology – Security techniques – Information security management guidelines for telecommunications organizations based on ISO/IEC 27002"

ITU-T X.1055

"Risk management and risk profile guidelines for telecommunications organizations"

ITU-T X.1056

"Security incident management guidelines for telecommunications organizations"

ITU-T X.1081

"The telebiometric multimodal model – A framework for the specification of security and safety aspects of telebiometrics"

ITU-T X.1082

"Telebiometrics related to human physiology"

ITU-T X.1083

"Information technology – Biometrics – BioAPI interworking protocol"

ITU-T X.1084

"Telebiometrics system mechanism – Part 1: General biometric authentication protocol and system model profiles for telecommunications systems"

ITU-T X.1086

"Telebiometric protection procedure – Part 1: A guideline to technical and managerial countermeasures for biometric data security"

ITU-T X.1088

"Telebiometrics digital key framework (TDK) – A framework for biometric digital key generation and protection"

ITU-T X.1089

"Telebiometrics authentication infrastructure (TAI) "

ITU-T X.1111

"Framework for security technologies for home network"

ITU-T X.1112

"Device certificate profile for the home network"

ITU-T X.1113

"Guideline on user authentication mechanism for home network services"

ITU-T X.1114

"Authorization framework for home network"

ITU-T X.1121

"Framework of security technologies for mobile end-to-end data communications"

ITU-T X.1122

"Guideline for implementing secure mobile systems based on PKI"

ITU-T X.1123

"Differentiated security service for secure mobile end-to-end data communication"

ITU-T X.1124

"Authentication architecture for mobile end-to-end data communication"

ITU-T X.1125

"Correlative Reacting System in mobile data communication"

ITU-T X.1141

"Security Assertion Markup Language (SAML 2.0)"

ITU-T X.1142

"Web services security – eXtensible Access Control Markup Language (XACML 2.0)"

ITU-T X.1143

"Security architecture for message security in mobile web services"

ITU-T X.1151

"Guideline on secure password-based authentication protocol with key exchange"

ITU-T X.1152

"Secure end-to-end data communication techniques using trusted third party services"

ITU-T X.1161

"Framework for secure peer-to-peer communications"

ITU-T X.1162

"Security architecture and operations for peer-to-peer network"

ITU-T X.1171

"Threats and requirements for protection of personally identifiable information in applications using tag-based identification"

ITU-T X.1191

"Functional requirements and architecture for IPTV security aspects"

ITU-T X.1205

"Overview of cybersecurity"

ITU-T X.1206

"A vendor-neutral framework for automatic notification of security related information and dissemination of updates"

ITU-T X.1207

"Guidelines for telecommunication service providers for addressing the risk of spyware and potentially unwanted software"

ITU-T X.1231

"Technical strategies for countering spam"

ITU-T X.1240

"Technologies involved in countering email spam"

ITU-T X.1241

"Technical framework for countering email spam"

ITU-T X.1242

"Short message service (SMS) spam filtering system based on user-specified rules"

ITU-T X.1244

ITU-T "Overall aspects of countering spam in IP-based multimedia applications"

ITU-T X.1303

"Common alerting protocol (CAP 1.1)"

Resolution 45 of the ITU World Telecommunication Development Conference (Doha, 2006)

"Mechanisms for enhancing cooperation on cybersecurity, including combating spam"

Recommendation ITU-R M.1078

"Security principles for IMT-2000"

Recommendation ITU-R M.1223

"Evaluation of security mechanisms for IMT-2000"

Recommendation ITU-R M.1457

"Security mechanisms incorporated in IMT-2000"

Recommendation ITU-R M.1645

"Framework and overall objectives of the future development of IMT-2000 and systems beyond IMT-2000"

Recommendation ITU-R S.1250

"Network management architecture for digital satellite systems forming part of SDH transport networks in the fixed satellite service"

Recommendation ITU-R S.1711

"Performance enhancements of transmission control protocol over satellite networks"

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

cybersecurity@itu.int
www.itu.int/cybersecurity