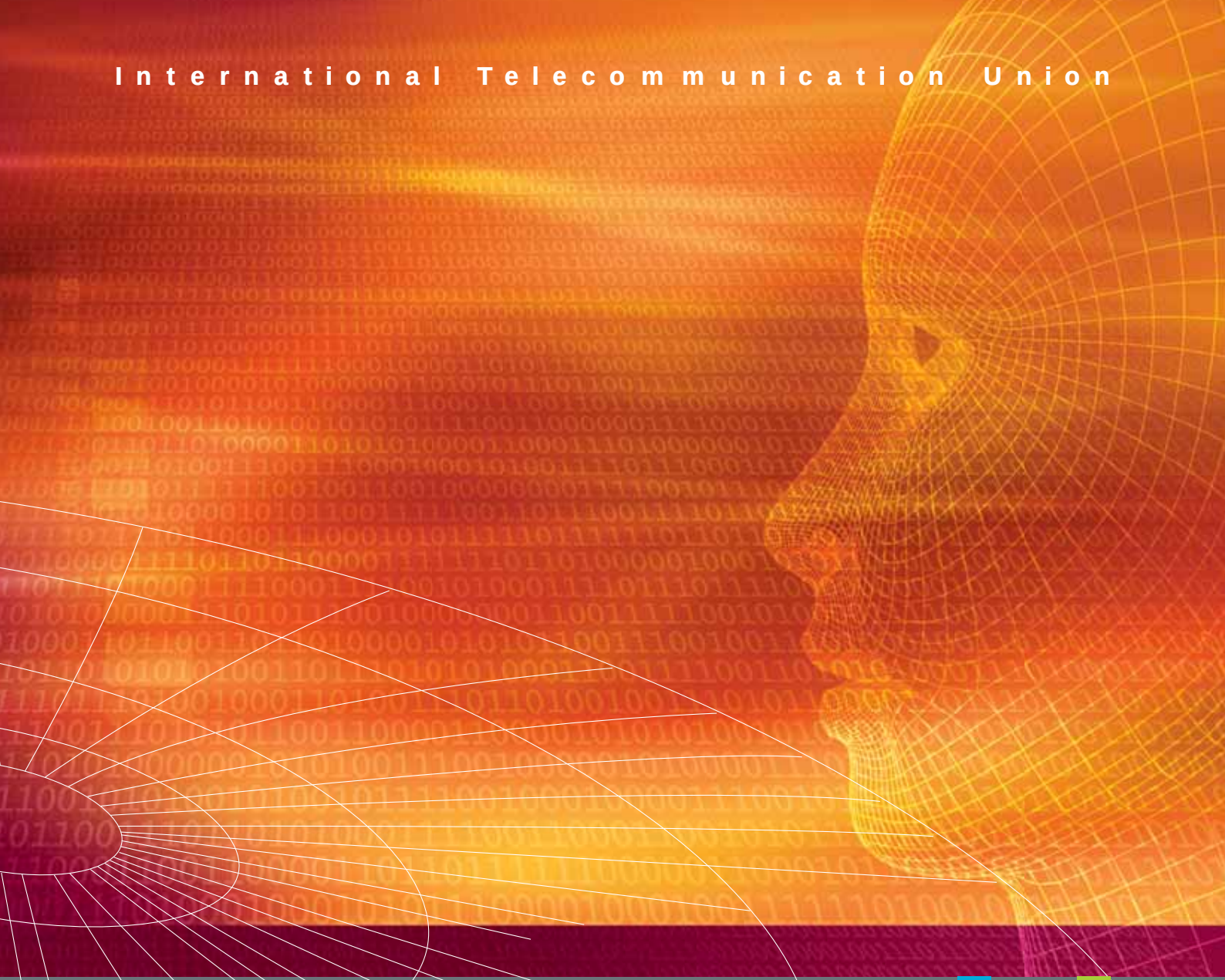
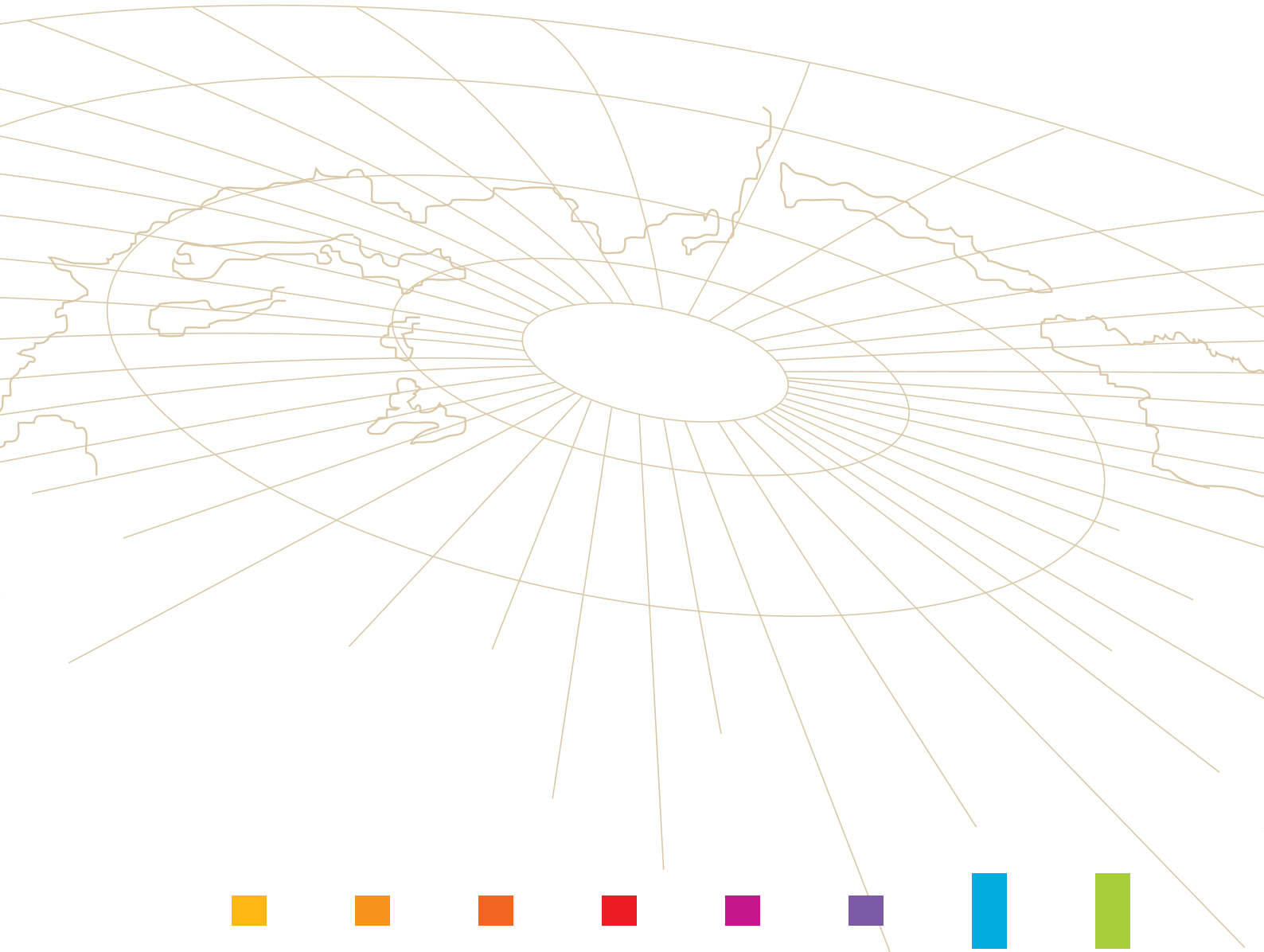
International Telecommunication Union



Cybersecurity for ALL

ITU's Work for a Safer World

International Telecommunication Union



Cybersecurity for ALL

ITU's Work for a Safer World

International Telecommunication Union

Message from ITU

Secretary-General, Dr Hamadoun I. Touré

The estimated number of Internet users worldwide exceeded the one billion mark in 2006, with the number of subscribers with access at broadband speeds surpassing one quarter of a billion. As the number of Internet users and the size, scope and power of the network grow, so too do the threats and risks associated with online access. Cyberthreats have evolved from annoying nuisances into something more menacing, with the availability to wreak havoc on our critical network infrastructures, as well as the data and information transmissions they carry. Cyberattacks (including viruses, worms, identity theft and Denial of Service attacks) can now be executed from anywhere, at any time, causing massive damage in a matter of minutes.

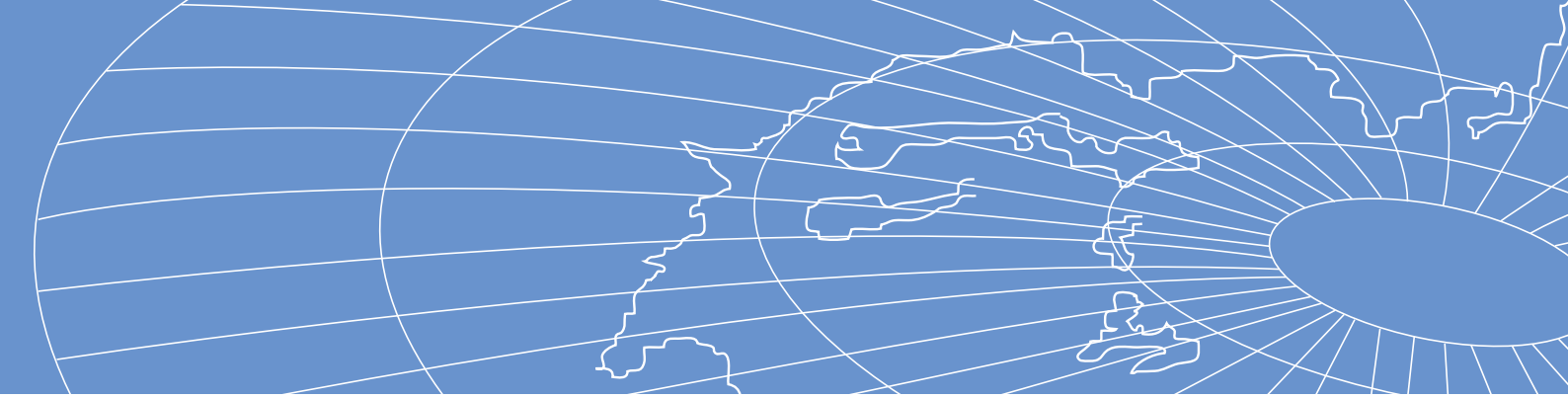
The threat concerns us all. At work, we may be entrusted with sensitive corporate data. At home, we may be anxious to ensure that our children can surf the web safely, free from molestation. In our digital transactions, we may be concerned with the confidentiality of our correspondence and freedom from email surveillance. As consumers, we may be worried about the security of online payments and our credit card details. Cybersecurity is a complex issue that affects us all, in all our different capacities and activities online.

As the oldest member of the UN family, ITU has a long history of promoting safe and secure communications. ITU is working hard to address the new and emerging challenges of the Information Society, notably in building confidence and trust in the use of Information and Communications Technologies (ICTs). The World Summit on the Information Society (WSIS), a UN Summit held in two phases in Geneva in 2003 and Tunis in 2005, entrusted ITU with the mandate to coordinate the efforts of all stakeholders in this field. Accordingly, ITU is undertaking a range of activities - from seeking international consensus on a multilateral framework for global cybersecurity, to working to develop and

implement the standards essential for the safe adoption and use of new technologies, to working with developing countries to raise awareness, build capacity and fulfill their specific needs for reliable, safe and secure communications. The ITU has launched a major new initiative, the Global Cybersecurity Agenda (GCA), as a global framework for 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 in five main work areas: legal measures, technical and procedural measures, organizational structures, capacity-building and international cooperation.

Much has been achieved. Much more remains to be done. We are confident, however, that together, we can build confidence and trust in the use of ICTs to make the online world safer and more secure.

Dr Hamadoun I. Touré
Secretary-General of the International Telecommunication Union (ITU)



2.

Foreword by the 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 traveled 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 is 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

3. Introduction

A battle for the future integrity of the Internet is underway. From its origins as a private, secure defense research network, the Internet has transformed modern lifestyles with its promise of real-time communications and limitless information. And yet, at the same time, the rapid growth of ICT networks has also opened up new opportunities for criminals to exploit online vulnerabilities and attack countries' critical infrastructure. Confidence and security in using ICTs are vital for building an inclusive, secure and global Information Society, as acknowledged by the World Summit on the Information Society (WSIS), but the future growth and potential of the online environment are in danger from growing cyberthreats.

The Internet began as a closed network with a limited number of trusted users, meaning that user authentication was not originally a major issue. In today's open Internet, where anyone with access to an Internet café can log on, online identity – and conversely, online anonymity – is a key issue. We have reached a point where no sooner is a new device or technology introduced, than hacker websites spring up to exchange ideas and approaches seeking to compromise the new technology. The constant evolution in protocols means that the protocols and algorithms used to secure Internet transactions are successively compromised and replaced, in a constant tug-of-war of human ingenuity.

Organizations and individuals are increasingly dependent on the information stored and transmitted over advanced communications and computer networks. Network security is vitally important: we rely on the smooth and secure functioning of networks in our online activities at work, at home and as consumers. This has led to a heightened awareness of the need to protect critical data and resources. Failure to address security issues can not only leave service

providers vulnerable to attacks in denial of service and/or network outages, it can also give rise to substantial losses and damage to firms' confidential data and business systems. The costs can be significant – in terms of lost revenue, loss of sensitive data and damage to equipment, as well as less easily replaced loss of reputation and standing with customers.

The ITU is working hard to address these emerging challenges of the Information Society and is developing an international framework to address threats to cybersecurity. ITU is promoting cybersecurity through a range of activities related to standardization and technical assistance to developing countries tailored to their specific needs. ITU is made up of three Sectors: the Radiocommunication Sector (ITU-R), the Standardization Sector (ITU-T) and the Telecommunication Development Sector (ITU-D). The work of these three Sectors is highlighted in Sections 5 and 6. In addition, there are some important initiatives being undertaken by the Secretary-General, which are highlighted in Section 4.

At the World Summit on the Information Society (WSIS), world leaders and governments entrusted ITU to take the lead in coordinating international efforts in this field, as the sole Facilitator of Action Line C5, "Building confidence and security in the use of ICTs". This is a responsibility that the ITU takes very seriously: the ITU is deeply committed through a range of activities to helping ensure that communications over public telecommunication networks remain secure, reliable and user-friendly.

world summit
on the **information society**
Geneva 2003 - Tunis 2005

4.

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

On 17 May 2007, ITU launched the Global Cybersecurity Agenda (www.itu.int/cybersecurity/) to provide a framework within which the international response to the growing challenges to cybersecurity can be coordinated and addressed. The ITU Secretary-General will benefit from the advice of an expert panel on the complex issues surrounding cybersecurity. The High-Level Experts Group consists of world-renowned specialists in cybersecurity, representing expertise from across a broad range of backgrounds in policy-making, government, academia and the private sector. This advisory Group met for the first time in Geneva on 5 October 2007 to develop concrete strategies to combat cybercrime and promote cybersecurity. The High-Level Experts Group will formulate proposals to the ITU Secretary-General on possible long-term strategies to promote cybersecurity in five key work areas (Figure 1) or pillars:

1. **Legal measures:** this work area focuses on key legal challenges and how best to coordinate legislation. It will develop guidance as to how criminal activities committed through computer networks can best be dealt with through legislation in an internationally compatible manner. This work area will develop model cybercrime legislation that is interoperable with existing national and regional legislative measures and consider how best to deal with loopholes in current legal frameworks that allow criminals to operate between countries with impunity.

2. **Technical and procedural measures:** this work area will focus on the key technical challenges arising to cybersecurity. Cyberthreats are constantly being developed to exploit technical vulnerabilities in ICT services and applications to gain unauthorized access to information and

communication systems. Security vendors and software manufacturers work continuously to identify, resolve and address weaknesses in their products. This work area focuses on technical and procedural measures for addressing vulnerabilities in software products, including accreditation schemes, protocols and standards.

3. **Organizational structures:** Countries' ability to monitor, prevent and deal with cyberattacks depends in large part on the watch, warning and response systems and capacity that they have established. This work area will focus on optimal response strategies and the institutions that can help countries in dealing with prevention, detection, response to and crisis management of cyberattacks, including the protection of countries' critical information infrastructure systems. This work area should develop a generic framework for functional organizational structures that can help countries deal with cyberthreats and the misuse of ICTs for malicious purposes.

4. **Capacity-Building**: this work area focuses on elaborating strategies for concrete capacity-building mechanisms that can be adopted to raise awareness, transfer know-how and boost cybersecurity on the national policy agenda. User awareness, technical capacity and information exchange are some of the key factors in building cybersecurity from the grassroots upwards. This work area will consider the effective measures, awareness campaigns and training initiatives that can be undertaken to build human, technical and institutional capacity and awareness of the issues key to promoting cybersecurity.

5. **International Cooperation:** this work area will develop proposals on a framework for a multi-stakeholder strategy for international cooperation, dialogue and coordination in dealing with cyberthreats. The Information Society is borderless, which means that the response mechanisms dealing with cyberthreats must be as borderless as cybercriminals' activities. Cooperation is vital at different levels and through different means – from the monitoring of funds and the transfers of the proceeds of criminal activities to cooperation in dealing with international crime syndicates and paedophilic rings.

Figure 1 illustrates the five work areas. The Global Cybersecurity Agenda represents a pioneering initiative by the ITU to develop a comprehensive multilateral framework for international cooperation to address new issues and promote cybersecurity.

Figure 1: ITU's Global Cybersecurity Agenda

5. Leading Work on Standards for Security

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.

Standardization can help guarantee established levels of performance and security in technologies, systems and products and help provide businesses with a systematic approach to information security. Manufacturers and service providers can be sure that their concerns have been reviewed in consultation with leading experts in the field in reaching the standard approach or processes needed to achieve minimum levels of performance. Standards help create confidence among providers and end-users that technologies and products have been tested and ensure a known level of performance.

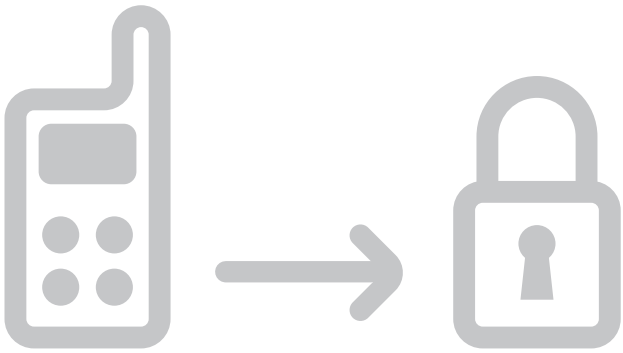
Standards development bodies have a vital role to play in addressing security vulnerabilities in protocols. As well as many key security Recommendations, ITU has developed overview security requirements, security guidelines for protocol authors, guidance on how to identify cyberthreats and countermeasures to mitigate risks. 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, tele-biometrics for authentication, security for emergency telecommunications and telecommunication network security requirements (Figure 2). 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 cyberattacks.

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

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

"Standardization is a key building block in constructing a global culture of cybersecurity. We can and will win the war against cyber-threats. We will do so by building on the work of the thousands of dedicated individuals—from governments, the private sector and civil society—who come together, in organizations like ITU, to develop security standards and guidelines for best practices."



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.

Currently, all ITU Study Groups conduct security-related activities and review security questions as part of their work, while Study Group 17 acts as the overall Lead Study Group on Communications System Security (Box 1). 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 (Box 2).

Box 1: The work of ITU-T Study Group 17

Study Group 17 is the Lead Study Group on Communications System Security and handles security guidance and the coordination of security-related work across all ITU-T Study Groups. It is responsible for studies on security, the application of open system communications (including networking and directory), technical languages and other issues related to the software aspects of telecommunication systems. Its role as the Lead Study Group on work related to security was confirmed by the ITU-T Assemblies in 2000 and 2004, in close collaboration with ISO/IEC, as a tripartite joint action.

Study Group 17 has approved over one hundred Recommendations on security for communications, mainly in the X series of Recommendations (Figure 2), either by itself, or jointly with ISO/IEC. It regularly publishes a Security 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).

Study Group 17 also publishes a Security Compendium electronically on its website containing a catalogue of approved ITU-T Recommendations related to security and presenting an extract of ITU-T security definitions and definitions from other sources. The role of Study Group 17 was reinforced by various Resolutions adopted at the World Telecommunication Standardization Assembly in Florianopolis in 2004:

- Resolution 50 on "Cybersecurity" guiding ITU-T work to build Recommendations sufficiently robust to prevent exploitation by malicious parties;
- Resolution 51 on "Combating Spam";
- Resolution 52 on "Countering Spam by Technical Means", seeking to integrate the technical means to combat spam into the work of ITU-T Study Groups and SG 17 Recommendations.

Source: www.itu.int/ITU-T/studygroups/com17/index.asp. The Security Compendium is available online at www.itu.int/itudoc/itu-t/com17/activity.

Box 2: The ICT Security Standards Roadmap promoting collaboration between international standards bodies

The Roadmap was launched by ITU-T 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:

1. Part 1: ICT Standards Development Organizations and Their Work;
Part 1 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 and IEEE), complete with links to existing glossaries of security.

2. Part 2: Approved ICT Security Standards
Part 2 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.

3. Part 3: Security standards under development
Part 3 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.

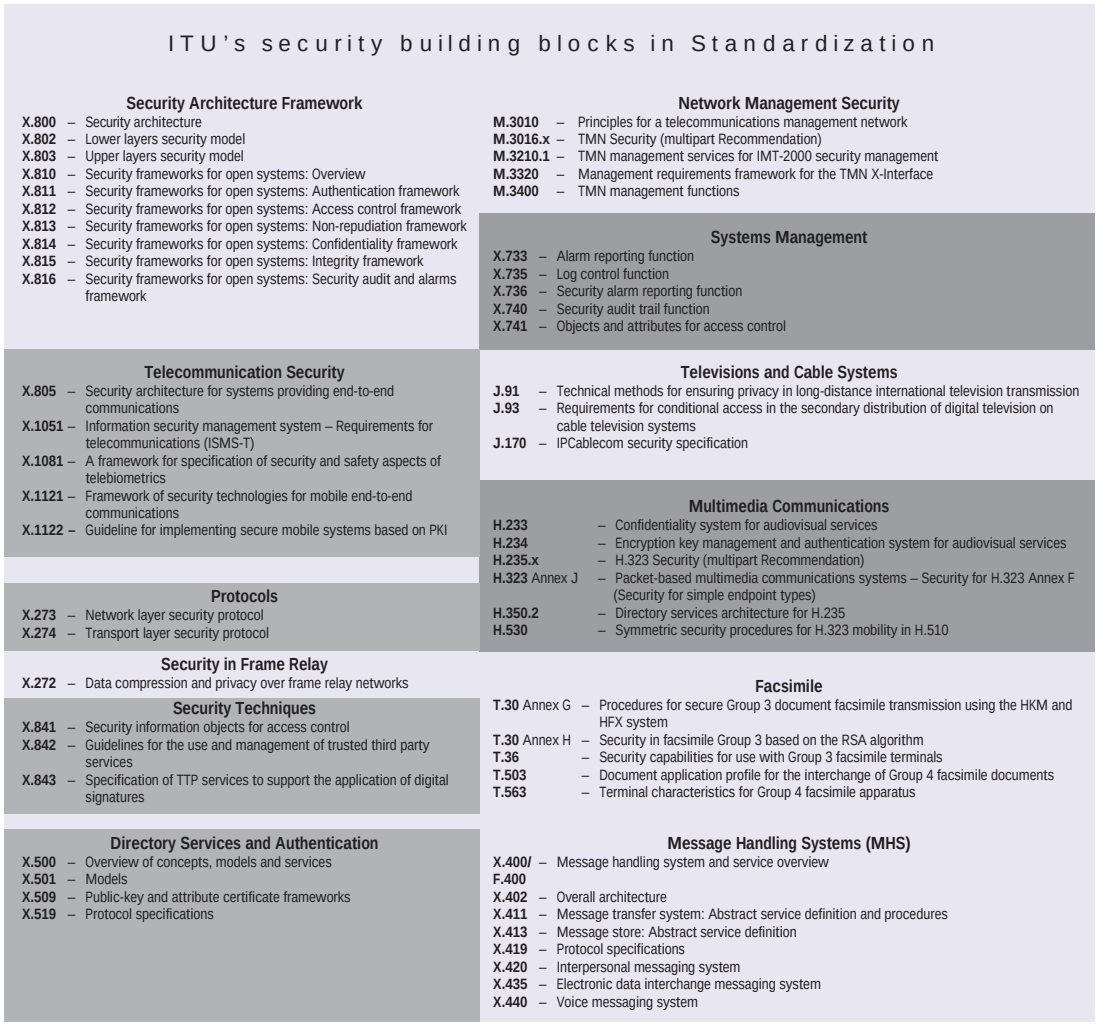
4. Part 4: Future needs and proposed new security standards
Part 4 will outline future areas of work in security standards, where gaps have been identified or proposals made for new standards work.

5. Part 5: Best practices
Part 5 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.

Source: www.itu.int/ITU-T/studygroups/com17/ict/index.html.

Figure 2: ITU's Security Building Blocks in Standardization



ITU-T Recommendations are available at http://www.itu.int/publications/bookshop/how-to-buy.html
(this site includes information on limited free access to ITU-T Recommendations).

Current important security work in ITU-T includes

Telebiometrics, Security management, Mobility security, Cybersecurity, Home-networking security, NGN security, Countering spam, Emergency telecommunications

For further information on ITU-T and its Study Groups: http://www.itu.int/ITU-T

6.

Security in Radiocommunications

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 Recommendation on "Security and Encryption for H-Series Multimedia Systems" 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.325 standard provides 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.325 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 has also issued recommendations on security issues in network management architecture for digital satellite systems (S.1250) and performance enhancements of transmission control protocol over satellite networks (S.1711).

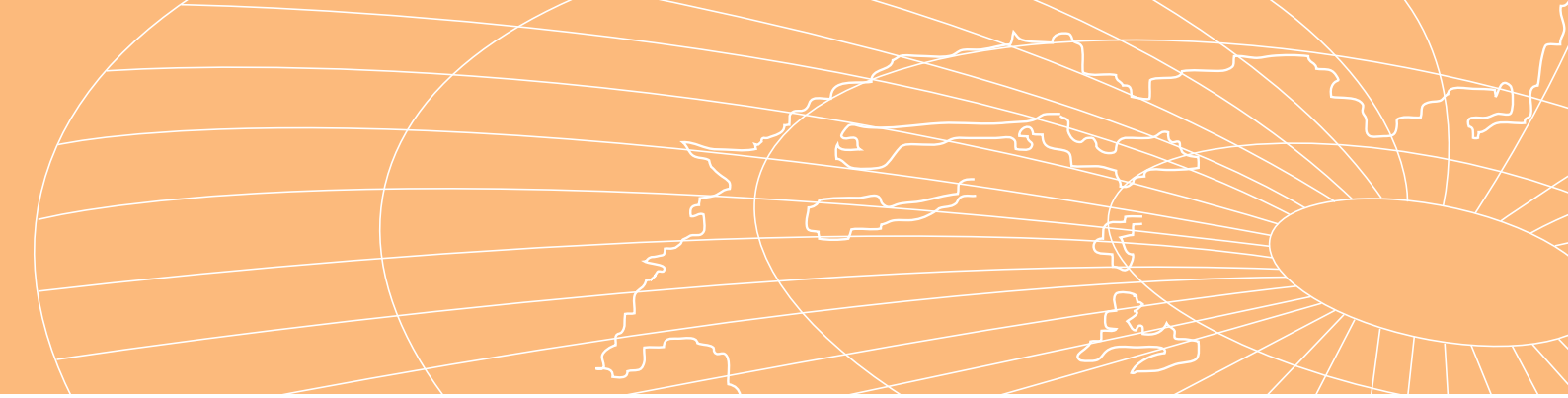
Safeguarding quality of service against degradation or denial of service is vital for the secure functioning of networks in data

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 standardization continues, matching the constant evolution in modern telecommunication networks. ITU-R established clear security principles for IMT-2000 (3G) networks (Recommendation 1078). ITU recommended early on that the security provided by mobile broadband IMT-2000 (3G) networks should be comparable to contemporary fixed networks.

Mr Valery Timofeev
Director, ITU Radiocommunication Bureau (BR)

"Cybersecurity represents an important element in several areas of ITU-R's activities. For the fixed-satellite service, security aspects are addressed in Recommendations concerning network management architecture and transmission control protocol, while security mechanisms are found in Recommendations concerning future land-mobile communications. Considerations of security are also a major feature in the development of evolving technologies such as software defined radio. With such examples, ITU-R is playing its part in the Union's overall thrust towards combating cyber-crime."



7. Security in ICT Development

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. National frameworks and strategies are needed that allow stakeholders to use all the technical, legal and regulatory tools available in promoting a culture of cybersecurity. While some countries are advanced in the formulation of national cybersecurity and Critical Information Infrastructure Protection (CIIP) strategies, others are only just beginning to consider the necessary measures to undertake.

Developing countries, with limited human, institutional and financial resources, face particular challenges in elaborating and implementing national policies and frameworks for cybersecurity and CIIP. For this reason, at the World Telecommunication Development Conference 2006 held in Doha, Qatar, cybersecurity was designated as a top priority for the ITU Telecommunication Development Sector (ITU-D) (www.itu.int/ITU-D/).

Practically, ITU's commitment in assisting developing countries is being implemented through two key and interrelated pillars. The first pillar is a new ITU Telecommunication Development Sector Study Group 1 Question 22 entitled *"Securing information and communication networks: Best practices for developing a culture of cybersecurity"* (www.itu.int/ITU-D/). In this activity, ITU is developing a *Report on Best Practices for a National Approach to Cybersecurity.* This Report outlines a *Framework for Organizing a National Approach to Cybersecurity* that identifies five key elements of a national effort, including:

1) Developing a national cybersecurity strategy;

2) Establishing national government-industry collaboration;

3) Creating a national incident management capability;

4) Deterring cybercrime; and

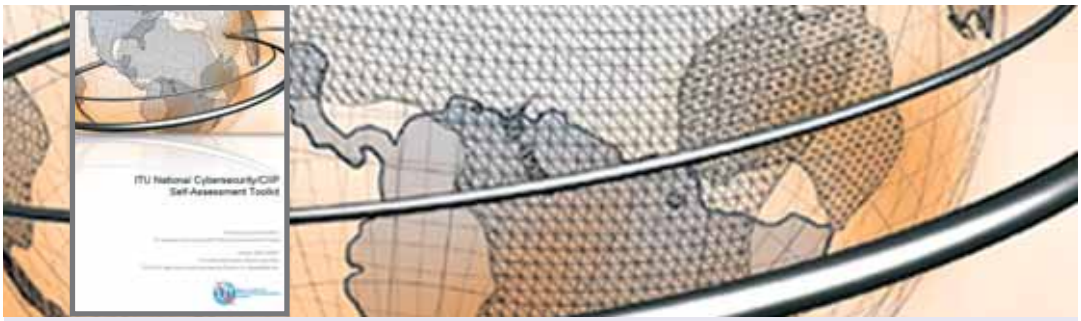
5) Promoting a national culture of cybersecurity.

The *Framework* identifies the main policy objectives, goals, and specific steps required for an effective national effort for each of the five elements, as well as resources and materials that can be drawn upon in developing and implementing each element.

Mr Sami Al Basheer Al Morshid

Director, ITU Telecommunication Development Bureau (BDT)

"With poor connectivity to the Internet backbone and limited technical and human resources, developing countries are particularly vulnerable to cybersecurity threats and attacks. We need international cooperation to help developing countries prevent, prepare for, protect against, respond to, and recover from cybersecurity incidents."



Box 3: ITU Toolkit to Assess National Cybersecurity/CIIP Readiness

Representing one of the key synergies between ITU-D Study Group Q22/1 work on "Securing information and communication networks: Best practices for developing a culture of cybersecurity" and the ITU Cybersecurity Work Programme for Developing Countries activities, the ITU National Cybersecurity/CIIP Self-Assessment Toolkit applies the framework under development in the Study Group with a practical toolkit for consideration at the national level. The toolkit assists governments in examining existing national policies, procedures, norms, institutions and other elements necessary for formulating security strategies in an ever-changing ICT environment. It helps governments better understand existing systems, identify gaps that require special attention and prioritize national response efforts. It addresses both policy and management layers, necessary institutions, as well as the relationships among government, industry and other private-sector entities.

The draft toolkit includes an Annex on Deterring Cybercrime: Substantive, Procedural and Mutual Assistance Law Baseline Survey intended to assist national authorities in reviewing their domestic situation related to the goals and actions identified in United Nations Resolutions 55/63 and 56/121 on Combating the Criminal Misuse of Information Technologies and the Council of Europe's Convention on Cybercrime.

Updates on the toolkit are continuously shared through the ITU-D cybersecurity website (www.itu.int/ITU-D/). Pilot country projects to test and evaluate the toolkit are being undertaken in conjunction with a number of regional capacity-building workshops organized by ITU. Countries interested in hosting a regional cybersecurity/CIIP capacity-building event or participating in a national cybersecurity/CIIP self-assessment initiative can contact cybmail@itu.int for further information.

Source: www.itu.int/ITU-D/cyb/cybersecurity/projects/readiness.html

The second pillar is the *ITU Cybersecurity Work Programme for Developing Countries* which sets out a detailed agenda for how ITU plans to assist Member States in developing cybersecurity capacities during the 2007-2009 timeframe. These cybersecurity and CIIP development initiatives include: helping countries increase basic cybersecurity/CIIP awareness; building human and national institutional capacities; assistance in development of sound national policies and enforceable legislation; expanding watch, warning and incident response capabilities; countering spam and related threats; conducting national self-assessments of cybersecurity/CIIP preparedness; and promoting the sharing of experiences between and amongst developing and developed countries. ITU is working with many partners from the public and private sectors on specific projects in all of these areas to assist developing countries.

Box 4: ITU Botnet Mitigation Toolkit

Botnets (also called zombie armies or drone armies) are networks of compromised computers infected with viruses or malware to turn them into "zombies" or "robots" — computers that can be controlled without the owners' knowledge. Criminals can use the collective computing power of these externally-controlled networks for malicious purposes and criminal activities, including generation of spam e-mails, launching of Distributed Denial of Service (DDoS) attacks (e.g., for blackmail purposes), alteration or destruction of data and identity theft.

An underground economy has sprung up around botnets, yielding significant revenues for authors of computer viruses, botnet controllers and criminals who commission this illegal activity by renting botnets.

The threat from botnets is growing fast. The latest (2007) generation of botnets (such as Zhelatin/Storm Worm) uses particularly aggressive techniques such as fast-flux networks and DDoS attacks against security vendors.

In response to this, ITU is developing a Botnet Mitigation Toolkit to help deal with the growing problem of botnets. The toolkit draws on existing resources, identifies relevant local and international stakeholders and takes into account the specific constraints of developing economies. The toolkit seeks to raise awareness among Member States of the growing threats posed by botnets and their linkages with criminal activities and incorporates the policy, technical and social aspects of mitigating the impact of botnets. The first draft of the toolkit will be made available in December 2007, with pilot tests planned in a number of Member States in 2008. Please contact cybmail@itu.int for more information about the toolkit.

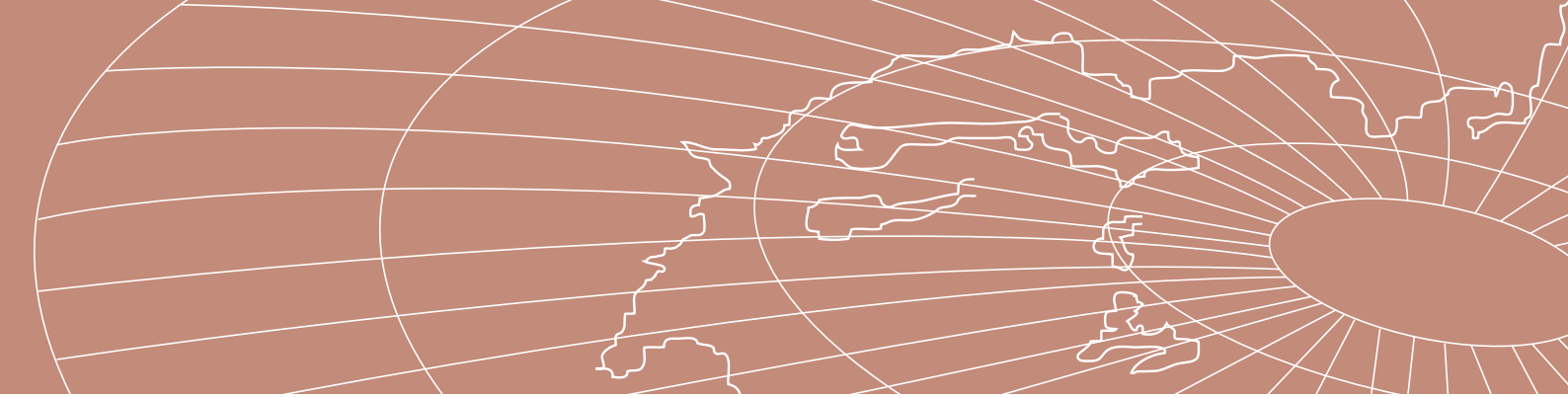
Source: www.itu.int/ITU-D/cyb/cybersecurity/projects/botnet.html

Box 5: ITU Toolkit for Model Cybercrime Legislation

Representing one of the five elements identified in the ITU-D Study Group Q22/1 developed Framework for Organizing a National Approach to Cybersecurity, deterring cybercrime is an integral component of a national cybersecurity/CIIP strategy. In particular, this includes the adoption of appropriate legislation against the misuse of ICTs for criminal or other purposes and activities intended to affect the integrity of national critical infrastructures. As threats can originate anywhere around the globe, the challenges are inherently international in scope and it is desirable to harmonize legislative norms as much as possible to facilitate regional and international cooperation.

The ITU Toolkit for Model Cybercrime Legislation aims to provide countries with model legislation that can assist in the establishment of a legislative framework to deter cybercrime. Development of the toolkit is being undertaken by a multidisciplinary international group of experts and a first draft will be made available in the first quarter of 2008. Please contact cybmail@itu.int for more information about the toolkit.

Source: www.itu.int/ITU-D/cyb/cybersecurity/projects/cyberlaw.html



8

Working Towards a More Secure Future

As the use of ICTs has grown and become more pervasive, and as our dependence on ICTs has increased, so too have the threats and risks associated with the Information Society and online world. At the World Summit on the Information Society (WSIS), world leaders and governments entrusted ITU to take the lead in coordinating international efforts in this field, as the sole Facilitator of Action Line C5, “Building confidence and security in the use of ICTs”. ITU takes this responsibility very seriously and is committed through a range of activities to helping ensure that communications over public telecommunication networks remain secure, reliable and user-friendly.

ITU is working hard to address the emerging challenges of the Information Society and is developing an international framework to address threats to cybersecurity. ITU is promoting cybersecurity through a range of activities related to standardization and technical assistance to developing countries tailored to their needs. Threats to the Information Society are constantly evolving, but we have every confidence that, united, we can work together to make the Information Society safer and more secure.

9. List of Acronyms

ATIS	Automatic Terminal Information Service
CERT	Computer Emergency Readiness Team
CIIP	Critical Information Infrastructure Protection
DDOS	Distributed Denial of Service
ENISA	European Network and Information Security Agency
ETSI	International Electrotechnical Commission
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
IMT-2000	International Mobile Telecommunications-2000
IP	Internet Protocol
ISO	International Organization for Standards
ITU	International Telecommunication Union
NGN	Next-Generation Networks
NISSG	Network and Information Security Steering Group
OAIS	Open Archival Information System
PKI	Public Key Infrastructure
QoS	Quality of Service
UN	United Nations
WSIS	World Summit on the Information Society
WTSA	World Telecommunication Standardization Assembly

"Global Cybersecurity Agenda", ITU (2007), Geneva, available from **www.itu.int/cybersecurity/gca/**

Photo credits

Pages 3, 5, 13, 17, 21: © ITU/J. M. Ferré

Pages 6, 9, 14, 23: © PhotoDisc

International Telecommunication Union

International Telecommunication Union

Corporate Strategy Division

Place des Nations

CH-1211 Geneva 20

Switzerland

Email: strategy@itu.int

www.itu.int/cybersecurity

04/2008

Printed in Switzerland
Geneva, 2008