Council2008
Geneva, 13-21 November 2008

Agenda item: PL XXX

C08/33-E
12 November 2008
Original: English

Some Proposals from HLEG taken into account by ITU Secretary General based on feedback by Sector Focal Points

ITU ACTIVITIES ON CYBERSECURITY IN RELATION TO THE GLOBAL CYBERSECURITY AGENDA (GCA)

WORK AREA 1 – LEGAL MEASURES	**RELEVANT ITU MANDATE**
1.1. ITU is a leading organisation of the United Nations system for the development of the main strategic goal of the GCA for legislative measures, and could elaborate strategies for the development of model legislation on cybercrime and other information security and network security issues as guidelines that are globally applicable and interoperable with existing national and regional legislative measures.	**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) *d)* Recognizing that "ICTS can be used to promote economic growth and enterprise development. Infrastructure development, human capacity building, information security and network security are critical to achieve these goals. We further recognise the need to effectively confront challenges and threats resulting from use of ICTS for purposes that are inconsistent with objectives of maintaining international stability and security and may adversely affect the integrity of the infrastructure within States, to the detriment of their security. It is necessary to prevent the abuse of information resources and technologies for criminal and terrorist purposes, while respecting human rights". (Para 15 of the Tunis Commitment) **WSIS Action Line C5** "Promote cooperation among the governments at the United Nations and with all stakeholders at other appropriate for a to enhance user confidence, build trust, and protect both data and network integrity; consider existing and potential threats to ICTS; and address other information security and network security issues". (Para 12 a)
1.2. ITU could encourage governments to cooperate with other stakeholders to develop necessary legislation for the investigation and prosecution of cybercrime, noting existing frameworks: for example, United Nations General Assembly Resolutions 55/63 and 56/121 on "Combating the criminal misuse of information technologies" and regional relevant initiatives.	**Resolution 45 of the ITU World Telecommunication Development Conference (Doha, 2006)** "Mechanisms for enhancing cooperation on cybersecurity, including combating spam". (Para a point c) **Doha Action Plan Programme 3 of the ITU World Telecommunication Development Conference (Doha, 2006)** "Provide assistance to Member States in developing laws and model legislation for the prevention of cybercrime". (Para 2.3 c)

1.3.	ITU could assist countries in promoting legislative efforts against spam, identity theft, criminalization of preparatory acts prior to attempted acts, and massive and coordinated cyberattacks against the operation of critical information infrastructure.	**Resolution 51 of the ITU World Telecommunication Standardization Assembly (Florianópolis, 2004)** "Combating spam" **Doha Action Plan Programme 3 of the ITU World Telecommunication Development Conference (Doha, 2006)** "Provide assistance to Member States in developing laws and model legislation for the prevention of cybercrime". (Para 2.3 c)
1.4.	Given the ever-changing nature of ICTs, it is challenging for law enforcement in most parts of the world to keep up with criminals in their constant efforts to exploit technology for personnel and illegal gains. In view of this, ITU could play an important role in promoting close cooperation between police forces, government and other elements of the criminal justice system, Interpol and other international organizations, the public at-large, the private sector and non-governmental organizations to ensure the most comprehensive approach to the problem.	**Doha Action Plan Programme 3 of the ITU World Telecommunication Development Conference (Doha, 2006)** "This programme should also develop a common understanding of the issues of spam and cyberthreats, including countermeasures. To minimize, prevent and detect cyberthreats, it is also necessary to facilitate further outreach and cooperation in order to support the collection and dissemination of cybersecurity-related information, and to exchange good practices to support effective mutual assistance, response and recovery among ITU Members and between government, business and civil society." (Para 1 a)
1.5.	ITU could organize a global conference on building confidence and security in the use of ICTs with the participation of ITU Members, as well as, regional and international organizations on cybersecurity and relevant private organizations on cybercrime. Participating organizations may include, but not limited to: INTERPOL, United Nations Office on Drugs and Crime (UNODC), G 8 Group of States, Council of Europe, Organization of American States (OAS), Asia Pacific Economic Cooperation (APEC), The Arab League, The African Union, The Organisation for Economic Cooperation and	**Resolution 140 of the ITU Plenipotentiary Conference (Revised, Antalya, 2006)** Instructs the Secretary-General to take all the necessary measures for ITU to fulfil its role as leading facilitator for implementing Action Line C5**.** **Resolution 130 of the ITU Plenipotentiary Conference (Revised, Antalya, 2006)** **WSIS Action Line C5** "Building confidence and security in the use of information and communication technologies (ICTs)". Terms of reference of Action Line Facilitators

Development (OECD), The Commonwealth, European Union, Association of South East Asian Nations (ASEAN), North Atlantic Treaty Organization (NATO) and the Shanghai Cooperation Organization (SCO).	
WORK AREA 2 – TECHNICAL & PROCEDURAL MEASURES	**RELEVANT ITU MANDATE**
2.1. ITU can and should work with existing external centres of expertise to identify, promote, and foster adoption of enhanced security procedures and technical measures.	**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".
2.2. ITU should take steps to facilitate becoming the global "centre of excellence" for the collection and distribution of timely telecommunications/ ICT cybersecurity-related information including a publicly available institutional ecosystem of sources – necessary to enhance cybersecurity capabilities worldwide.	**Resolution 140 of the ITU Plenipotentiary Conference (Antalya, 2006)** ITU's role in implementing the outcomes of the World Summit on the Information Society. **ITU-T SG 17 Security Standards Roadmap Project:** This Roadmap is an on-line resource that provides information about existing ICT security standards and work in progress in key standards development organizations including ITU-T, ISO/IEC, ATIS, ENISA, ETSI, IEEE, IETF, OASIS, 3GPP, and 3GPP2.
2.3. ITU should collaborate with organizations, vendors, and other appropriate subject matter experts to (1) advance incident response as a discipline worldwide, (2) promote and support possibilities for Computer Security Incident Response Teams (CSIRTs) to join the existing global and regional conferences and forums, in order to build capacity for improving state-of-art incident response on a regional basis, and (3) collaborate in the development of materials for establishing national CSIRTs and for effectively communicating with the CSIRT authorities.	**Resolution 45 of the ITU World Telecommunication Development Conference (Doha, 2006)** "Mechanisms for enhancing cooperation on cybersecurity, including combating spam". **ITU-T Recommendation E.409** Incident organization and security incident handling: Guidelines for telecommunication organizations.

2.4.	ITU should establish a long-term commitment to develop and refine the efforts of Study Group 1/Question 22 to identify and promote best practices related to national frameworks for managing cybersecurity and Critical Information Infrastructure Protection (CIIP), as well as to establish regional workshops that help to identify and share techniques for establishing and maintaining comprehensive cybersecurity programmes.	**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".
2.5.	To promote more efficient approaches for improving security and risk management processes, HLEG recommends that any initiatives or recommendations in the field of technical measures must build upon the important work that has been done by ITU on the development of best practices and standards for cybersecurity.	**Doha Action Plan Programme 3 of the ITU World Telecommunication Development Conference (Doha, 2006)** Identify cybersecurity requirements and propose solutions for the development of secure ICT applications. Assist in raising awareness and identify key issues to support a culture of cybersecurity, and recommend models of good practice to support ICT applications and minimize cyberthreats. (Para 2.3. g) **ITU-T Recommendation X.1051** Information technology - Security techniques - Information security management guidelines for telecommunications organizations based on Information technology - Security techniques - Information security management guidelines for telecommunications organizations based on ISO/IEC 27002.
2.6.	ITU should undertake investigation, analysis, and selection (in cooperation with ITU-T, International Organization for Standardization (ISO), International Electrotechnical Commission (IEC), and other relevant bodies) of the ICT security standards and frameworks that can be leveraged to promote procedural measures. The frameworks to be investigated include ISO/IEC JTC 1/SC 27 standards and technical reports on security techniques, the IT Baseline Protection Manual (from Bundesamt für Sicherheit in der	**ITU-T X.500, X.800 and X.1000 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. **The Security Manual** "Security in telecommunications and information technology - An overview of issues and the deployment of existing ITU-T Recommendations for secure tele-

	Informationstechnik), the COBIT (from IT Governance Institute), ITU-T X-series Recommendations (developed by ITU-T SG 17), and other documents about security, evaluating and certification of information systems and network security.	communications".
2.7.	ITU should develop proposals for procedural measures based on the selected ICT security standards and frameworks. As there are many useful materials, the ITU proposal might concern application and promotion of existing standards and frameworks (or their combinations), instead of elaborating its own versions or standards.	**Resolution 7 of the ITU World Telecommunication Standardization Assembly (Florianópolis, 2004)** "Collaboration with the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC)". **ITU-T Recommendation A6** Cooperation and exchange of information between ITU-T and national and regional standards development organizations.
2.7.1	Internet – investigate ways to collaborate with private industry to enhance the security of public communication networks and ISPs. For example, the Trusted Service Provider (SPID) initiative, Domain Name System (DNS) Security Extensions (DNSSEC), or systemic and economic incentives for security for protection of global telecommunications, might be further examined and discussed. In collaboration with private industry, ITU may examine the role of Internet Service Providers (ISPs) in blocking spam and other issues. Particular attention should be paid to investigating theresults of SG 13 (ITU-T's largest and most active standards body that addresses global information infrastructure, internet protocol aspects and next-generation networks**,** and has engaged a broad, large cross section of global industry players and technical bodies).	**Resolution 50 of the ITU World Telecommunication Standardization Assembly (Florianópolis, 2004)** "Cybersecurity". **Resolution 51 of the ITU World Telecommunication Standardization Assembly (Florianópolis, 2004)** "Combating spam". **Resolution 52 of the ITU World Telecommunication Standardization Assembly (Florianópolis, 2004)** "Countering spam by technical means". **ITU-T Recommendation X.1205** "Overview of cybersecurity". **ITU-T Recommendation X.1231** "Technical strategies on countering spam". **ITU-T Recommendation X.1240** "Technologies involved in countering e-mail spam". **ITU-T Recommendation X.1241** "Technical framework for countering e-mail spam".

	ITU-T Recommendation X.509 "Public-key and attribute certificate frameworks (global standard on identity management)".
WORK AREA 3 – ORGANISATIONAL STRUCTURES	**RELEVANT ITU MANDATE**
3.1. ITU should undertake promotion of national cybersecurity policies in order to be able: • to address legal and organizational cybersecurity needs; • to build effective cybersecurity capacities; • to promote a national cybersecurity culture; • to promote the use of technical and procedural cybersecurity solutions; • to fight against cybersecurity incidents in a way that is effective at national level and compatible at regional and international level; • to raise awareness among citizens and all stakeholders; • to encourage cybersecurity education for all; • to encourage existing efforts and collaborative efforts; • to assist private and public partnerships.	**Doha Action Plan Programme 3 of the ITU World Telecommunication Development Conference (Doha, 2006)** "This programme should also develop a common understanding of the issues of spam and cyberthreats, including countermeasures. To minimize, prevent and detect cyberthreats, it is also necessary to facilitate further outreach and cooperation in order to support the collection and dissemination of cybersecurity-related information, and to exchange good practices to support effective mutual assistance, response and recovery among members and between government, business and civil society". (Para 1 a)
3.2. ITU could support national, regional and international strategies to fight against cybersecurity incidents in a global perspective.	**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".
3.3. ITU could encourage governments to continue to improve coordination at the national, regional and international levels in cybersecurity.	**Resolution 45 of the ITU World Telecommunication Development Conference (Doha, 2006)** "Mechanisms for enhancing cooperation on cybersecurity, including combating spam".
3.4. ITU could advise on appropriate organizational structures which would	**Resolution 2 of the ITU World Telecommunication Development Conference**

address countries' specific needs and should be adapted in regards of resources availability, private/public partnerships, ICT development, and ICT level of adoption of each country.	**(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".
3.5. ITU could encourage each country to develop its own strategy and organizational structures to address its national cybersecurity needs and should promote assistance through regional or international cooperation.	**Doha Action Plan Programme 3 of the ITU World Telecommunication Development Conference (Doha, 2006)** "…BDT should also act as a facilitator for regional and interregional cooperation, and support appropriate capacity-building activities at the regional level". (Para 1 a)
3.6. ITU should support the implementation of organizational structures and capacity-building needs in a gradual manner, depending on local factors.	**Doha Action Plan Programme 3 of the ITU World Telecommunication Development Conference (Doha, 2006)** "...BDT should also act as a facilitator for regional and interregional cooperation, and support appropriate capacity-building activities at the regional level". (Para 1 a)
WORK AREA 4 – CAPACITY BUILDING RECOMMENDATIONS	**RELEVANT ITU MANDATE**
4.1. ITU could have a lead role in coordinating robust, multi-stakeholder participation in cybersecurity investigation and solutions development and putting them into action, developing effective legal frameworks in the elaboration of strategies for the development of model cybercrime legislation as guidelines that are globally applicable and interoperable with existing national and regional legislative measures, in order to answer the needs identified in Work Area 1.	**Resolution 45 of the ITU World Telecommunication Development Conference (Doha, 2006)** "Mechanisms for enhancing cooperation on cybersecurity, including combating spam". **Doha Action Plan Programme 3 of the ITU World Telecommunication Development Conference (Doha, 2006)** "Provide assistance to Member States in developing laws and model legislation for the prevention of cybercrime". (Para 2.3 c) Explore opportunities for collaboration and work

		with identified potential partners, based on project requirements and recognized sources of expertise, and facilitating the creation of mutually beneficial and multi-stakeholder partnerships. (Para 2.5 a)
4.2.	ITU could promote the adoption and the support of technical and procedural cybersecurity measures in: (1) becoming the global 'centre of excellence' through collaboration with existing cybersecurity work outside ITU, (2) general procedural measures, (3) general technical measures, and (4) measures addressing specific technical topic, as specified by Work Area 2.	**Doha Action Plan Programme 3 of the ITU World Telecommunication Development Conference (Doha, 2006)** "…BDT should also act as a facilitator for regional and interregional cooperation, and support appropriate capacity-building activities at the regional level". (Para 1 a)
4.3.	ITU should support all Members in the development and promotion of national, regional and international policies and strategies to fight against cybersecurity incidents within a global perspective, including improving national, regional and international governments coordination in cybersecurity; encouraging a graduated response to organizational structures and capacity building needs (bearing in mind local factors); and helping to put in place organizational structures as presented in Work Area 3.	**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)** "...BDT should also act as a facilitator for regional and interregional cooperation, and support appropriate capacity-building activities at the regional level".
4.4.	ITU could assist in empowering end-users to adopt a safe behaviour in order to become responsible cyber-citizens.	**Doha Action Plan Programme 3 of the ITU World Telecommunication Development Conference (Doha, 2006)** Develop guidelines, planning tools and manuals on the technology and policy aspects of cybersecurity, internet protocol and ICT applications. (Para 2.1 a) Develop training materials on technology strategies and technology evolution for the implementation of cybersecurity, internet protocol and ICT applications. (Para 2.2)

4.5. ITU could promote the establishment of public-private partnerships when required in order: • To integrate security into infrastructure, • To promote a security culture, behaviour and tools, • To fight against cybercrime.	**Doha Action Plan Programme 3 of the ITU World Telecommunication Development Conference (Doha, 2006)** Identify cybersecurity requirements and propose solutions for the development of secure ICT applications. Assist in raising awareness and identify key issues to support a culture of cybersecurity, and recommend models of good practice to support ICT applications and minimize cyberthreats. (Para 2.3 g)
4.6. ITU could train and educate at several levels all the actors of the information society.	**Doha Action Plan Programme 3 of the ITU World Telecommunication Development Conference (Doha, 2006)** Develop guidelines, planning tools and manuals on the technology and policy aspects of cybersecurity, internet protocol and ICT applications. (Para 2.1 a) Develop cybersecurity, internet protocol and ICT applications toolkits for policy-makers and other relevant sectors. (Para 2.1 b) Develop training materials on technology strategies and technology evolution for the implementation of cybersecurity, internet protocol and ICT applications. (Para 2.2)
4.7. ITU should continue to develop human capacity in all aspects of cybersecurity to help build a global culture of cybersecurity: • By defining and publicizing an international day for "Internet security," to be woven into the fabric of national cybersecurity policies; • Through the creation and continuous maintenance of various resources to assist the countries to update their cybersecurity capacities; • Through the training of the minimum number of national decision-makers in the regions	**Doha Action Plan Programme 3 of the ITU World Telecommunication Development Conference (Doha, 2006)** Identify cybersecurity requirements and propose solutions for the development of secure ICT applications. Assist in raising awareness and identify key issues to support a culture of cybersecurity, and recommend models of good practice to support ICT applications and minimize cyberthreats. (Para 2.3 g)

that need international assistance with the aim to help all national governments have legal frameworks, technical and procedural measures, organizational structures and international cooperation frameworks by 2013; • By incorporating end-user cyberculture into the national cyber policy frameworks; • To establish a Global Fund, to be based on voluntary contributions, under ITU to address the need for various activities of the cybersecurity capacity building.	
WORK AREA 5 – INTERNATIONAL COOPERATION	**RELEVANT ITU MANDATE**
5.1. The ITU focal point for cybersecurity should be enhanced to manage the diverse activities in a coordinated manner in order to ensure successful execution of the ITU mandate. The focal point would also serve to ensure continuity in ITU after the HLEG has completed its work, and could identify priorities, follow up on implementation of the HLEG recommendations after their approval and, given the dynamism of the ICT environment, address new issues that arise after the completion of the work of the HLEG. This structural focal point would work with the global community on an ongoing basis to engage the existing international regional and national structures in building a common understanding of the relevant international issues, including the existing multiple threats to information security in accordance with the United Nations General Assembly Resolution 62/17 "Developments in the field of information and telecommunications in the context of international security" of December 5, 2007, and, as appropriate, develop compatible unified strategies and solutions. The functions of the structural focal point would include:	**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 of the Intersectoral objectives of the General Secretariat and in accordance with Article 11 of the Constitution and Article 5 of the Convention, 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". **WSIS Action Line C5** "Promote cooperation among the governments at the United Nations and with all stakeholders at other appropriate for a to enhance user confidence, build trust, and protect both data and network integrity; consider existing and potential threats to ICTS; and address other information security and network security issues". (Para 12 a) **Council 2007 Resolution 1282** ITU's role in implementing the outcomes of the World Summit on the Information Society.
5.1.1 To support and promote in international forums the ITU's activities in the development of technical standards to increase the security of networks (i.e., ITU-T activities) and ITU's activities in providing assistance to developing countries to protect their IP-based networks, through capacity building and providing information about national best practices (i.e., ITU-D activities);	**ISO/IEC/ITU-T** Strategic Advisory Group on security.
5.1.2 To support and promote the work of other organizations who have expertise in cybersecurity areas in which ITU does not have expertise, through such activities as information exchange, creation of knowledge, sharing of best practices, assistance in developing multi-stakeholder and public/private partnerships, collecting and publishing information, and maintaining a website;	**Doha Action Plan Programme 3 of the ITU World Telecommunication Development Conference (Doha, 2006)** "To minimize, prevent and detect cyberthreats, it is also necessary to facilitate further outreach and cooperation in order to support the collection and dissemination of cybersecurity-related information, and to exchange good practices to support effective mutual assistance, response and recovery among ITU Members and between government, business and civil society." (Para 1 a)
5.1.3 To work towards international harmonization of the activities of stakeholders in the various	**Resolution 71 of the ITU Plenipotentiary Conference (Antalya, 2006)**

fields of Cybersecurity, information security and network security issues;	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 140 of the ITU Plenipotentiary Conference (Antalya, 2006)** ITU's role in implementing the outcomes of the World Summit on the Information Society. **ITU role as sole moderator/facilitator for WSIS Action Line C5** **Resolution 130 of the ITU Plenipotentiary Conference (Revised, Antalya, 2006)** "..instructs the Director of the Telecommunication Development Bureau 5 to continue collaboration with relevant organizations with a view to exchanging best practices and disseminating information through, for example, joint workshops and training sessions. **WSIS Action Line C5** "Promote cooperation among the governments at the United Nations and with all stakeholders at other appropriate for a to enhance user confidence, build trust, and protect both data and network integrity; consider existing and potential threats to ICTS; and address other information security and network security

	issues". (Para 12 a)
5.1.4 To work with the global community on an ongoing basis to engage the existing international regional and national structures in building a common understanding of the international issues involving cybersecurity and developing unified strategies and solutions.	**Resolution 130 of the ITU Plenipotentiary Conference (Revised, Antalya, 2006)** "...instructs the Director of the Telecommunication Development Bureau 1 to develop, consistent with the results of WTDC-06 and the subsequent meeting pursuant to Resolution 45 (Doha, 2006) of that conference, the projects for enhancing cooperation on cybersecurity and combating spam responding to the needs of developing countries, in close collaboration with the relevant partners.
5.2. The ITU Secretary-General should initiate necessary activities, especially involving the many experts in the ITU sectors, combined with resources within the General Secretariat and the Bureau Directors and the many other cybersecurity-related bodies.	**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.
5.3. ITU should undertake general activities for the monitoring, coordination, harmonizing and advocating international cooperation.	**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 140 of the ITU Plenipotentiary Conference (Antalya, 2006)** ITU's role in implementing the outcomes of the World Summit on the Information Society. **ITU role as sole moderator/facilitator for WSIS Action Line C5** **Resolution 130 of the ITU Plenipotentiary Conference (Revised, Antalya, 2006)** "...instructs the Director of the Telecommunication Development Bureau 5 to continue collaboration with relevant organizations with a view to exchanging best practices and disseminating information through, for example, joint workshops and training sessions.