

## PROPOSAL 20

### **Resolution 130 of Marrakesh on the role of ITU in information and communication network security**

**Submitted by the following Member States:**

**Germany (Federal Republic of), Austria, Belarus (Republic of), Bulgaria (Republic of), Cyprus (Republic of), Spain, Estonia (Republic of), Finland, France, Lithuania (Republic of), Luxembourg, Norway, Netherlands (Kingdom of the), Poland (Republic of), Slovak Republic, Czech Republic, Romania, United Kingdom of Great Britain and Northern Ireland, Slovenia (Republic of), Sweden and Switzerland (Confederation of)**

#### **BACKGROUND**

**1. The Resolution 130 of PP-02 of Marrakech, the resolution 50 of WTSA 04 of Florianopolis on cybersecurity and the action plan of Doha**

The PP-02 of Marrakech adopted Resolution 130 on the role of ITU in information and communication network security; this resolution resolves “*to strengthen the role of ITU in information and communication network security*” and “*instructs the Secretary-General and the Directors of the Bureaux.*”

*1 to review ITU's current activities in information and communication network security;*

*2 to intensify work within existing ITU study groups in order to:*

- i) reach a common understanding on the importance of information and communication network security by studying standards on technologies, products and services with a view to developing recommendations, as appropriate;*
- ii) seek ways to enhance exchange of technical information in the field of information and communication network security, and promote cooperation among appropriate entities; »*

The WTSA of Florianopolis in 2004 also adopted resolution 50 on cybersecurity that

*“resolves*

*1 that ITU-T evaluate existing and evolving new Recommendations, and especially signalling and communications protocol Recommendations, with respect to their robustness of design and potential for exploitation by malicious parties to interfere*

*destructively with their deployment in the global information and communication infrastructure;*

*2 that ITU-T continue to raise awareness, within its area of operation and influence, of the need to defend information and communication systems against the threat of cyber attack, and continue to promote cooperation among appropriate entities in order to enhance exchange of technical information in the field of information and communication network security.”*

The World Telecommunication Development Conference of Doha in March 2006 adopted the Action Plan of Doha and its programme 3 on “e-strategies and ICTs applications”; this action plan identifies cybersecurity as a priority activity for BDT and states:

*“a) Cybersecurity: Enhance security and build confidence in the use of ICT applications*

*Security concerns have been identified as a barrier to the use of current and next generation networks for certain mission-critical services (e.g. e-commerce, e-governance, e-payment and e-health), where it is important to ensure confidentiality, integrity and availability of information systems. While the telecommunication network security concerns will be dealt with in Programme 2, it is necessary to address cybersecurity concerns in this programme in order to realize the potential of networks for providing secure and accessible e-service applications. This programme should also develop a common understanding of the issues of spam and cyber threats, including countermeasures. To minimize, prevent and detect cyber threats, 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.*

*BDT should also act as a facilitator for regional and interregional cooperation, and support appropriate capacity-building activities at the regional level.*

*This could include, inter alia, the development of MOUs among interested Member States to enhance cybersecurity.”*

Since PP02, a lot of work has been undertaken by ITU pursuant to these resolutions: different workshops on cybersecurity have been organized by ITU (SG, ITU-T, ITU-D) and standardization work has been achieved, especially by SG 17 of ITU-T.

Security is also a subject of major concern for European countries as recalled in different European Commission communications or by the Council of the European Union.

## **2. But new threats have emerged or developed since last PP02**

With the global development of the Internet, new significant and growing issues have developed: spam, phishing, malware, protection of personal data, privacy, intellectual property protection, fight against illicit content and so forth, that could threaten the security and stability of telecommunication networks.

The WTSA of Florianopolis in 2004 adopted two resolutions on the issue of spam: Resolution 51 on combating spam and Resolution 52 on countering spam by technical means.

The second phase of the WSIS of Tunis adopted the Agenda of Tunis that states

**“39. We seek** to build confidence and security in the use of ICTs by strengthening the trust framework. **We reaffirm** the necessity to further promote, develop and implement in cooperation with all stakeholders a global culture of cyber-security, as outlined in UNGA Resolution 57/239 and other relevant regional frameworks. This culture requires national action and increased international cooperation to strengthen security while enhancing the protection of personal information, privacy and data. Continued development of the culture of cyber-security should enhance access and trade and must take into account the level of social and economic development of each country and respect the development-oriented aspects of the Information Society.

**40. We underline** the importance of the prosecution of cybercrime, including cybercrime committed in one jurisdiction, but having effects in another. **We further underline** the necessity of effective and efficient tools and actions, at national and international levels, to promote international cooperation among, inter alia, law enforcement agencies on cybercrime. **We call upon governments** in cooperation with other stakeholders to develop necessary legislation for the investigation and prosecution of cybercrime, noting existing frameworks, for example, UNGA Resolutions 55/63 and 56/121 on "Combating the criminal misuse of information technologies" and regional initiatives including, but not limited to, the Council of Europe's Convention on Cybercrime.

**41. We resolve to deal effectively** with the significant and growing problem posed by spam. **We take note** of current multilateral, multi-stakeholder frameworks for regional and international cooperation on spam, for example, the APEC Anti-Spam Strategy, the London Action Plan, the Seoul Melbourne Anti-Spam Memorandum of Understanding and the relevant activities of OECD and ITU. **We call upon** all stakeholders to adopt a multi-pronged approach to counter spam that includes, inter alia, consumer and business education; appropriate legislation, law enforcement authorities and tools; the continued development of technical and self-regulatory measures; best practices; and international cooperation.

**42. We reaffirm our commitment** to the freedom to seek, receive, impart and use information, in particular, for the creation, accumulation and dissemination of knowledge. **We affirm** that measures undertaken to ensure Internet stability and security, to fight cybercrime and to counter spam, must protect and respect the provisions for privacy and freedom of expression as contained in the relevant parts of the Universal Declaration of Human Rights and the Geneva Declaration of Principles.

**44. We also underline** the importance of countering terrorism in all its forms and manifestations on the Internet, while respecting human rights and in compliance with other obligations under international law, as outlined in UNGA A/60/L.1\* with reference to Art. 85 of the 2005 World Summit Outcome.

**45. We underline** the importance of the security, continuity and stability of the Internet, and the need to protect the Internet and other ICT networks from threats and vulnerabilities. **We affirm** the need for a common understanding of the issues of Internet security, and for further cooperation to facilitate outreach, the collection and dissemination of security-related information and exchange of good practice among all stakeholders on measures to combat security threats, at national and international levels.

**46. We call upon all stakeholders to ensure respect for privacy and the protection of personal information and data, whether via adoption of legislation, the implementation of collaborative frameworks, best practices and self-regulatory and technological measures by business and users. We encourage all stakeholders, in particular governments, to reaffirm the right of individuals to access information according to Geneva Declaration of Principles and other mutually-agreed relevant international instruments, and to coordinate internationally as appropriate.”**

There is a need for a common understanding of these different issues, and for further cooperation to facilitate outreach and the collection and dissemination of best practices. There is also a need for developing or continuing the development of technical measures to protect telecommunication networks from these threats and vulnerabilities. ITU, as a unique intergovernmental organization with membership from both developed and developing countries, has a key role to play in these different activities.

## PROPOSALS

At the moment, there is only a PP-02 Resolution (Resolution 130) on cybersecurity. It would be necessary to have a resolution in order to address all the other issues highlighted above, inasmuch as they impact on the security of telecommunication networks.

In order to achieve this goal, there are different solutions: the first one would be to propose a resolution for each of the issues above; the second one would be to extend the scope of the Resolution 130 in order to address all the issues concerning the possible threats to the stability and security of networks.

As a principle of good governance, and in order to avoid the multiplication of resolutions, the second solution seems to be the better one.

A modified Resolution 130 is proposed as follows.

EUR/12/55

MOD

RESOLUTION 130 (Rev. Antalya, 2006)

### Role of the ITU in network security, including countering SPAM and other issues related to threats and vulnerabilities of ICT networks

Deleted: Marrakesh, 2002

Deleted: Strengthening the role of ITU in information and communication network security

The Plenipotentiary Conference of the International Telecommunication Union (Antalya, 2006),

Deleted: Marrakesh, 2002

*considering*

a) the crucial importance of information and communication infrastructures and their applications to practically all forms of social and economic activity;

b) that with the application and development of information and communication technologies (ICT), telecommunication networks have been faced with ever-growing security challenges,

Deleted: information and communication

Deleted: given rise to

c) that the variety, severity and number of network security incidents, including attacks from worms, viruses, etc. are on the increase;

d) that in the recent years, new threats have emerged like spam, malicious intrusions, fraudulent intrusions, etc., and that in years to come, other threats could emerge;

e) the need to facilitate, at the international level, the implementation of frameworks, best practices and technological measures to counter threats;

f) that there is a need for enhanced security options adapted to high level security requirements, and that new generation protocols and standards are being developed for this purpose;

g) the important role of the private sector in combating network security threats, in particular for the continued development of technical and self-regulatory measures and best practice;

h) that the Tunis Agenda for the Information Society urges relevant organizations to further promote, develop and implement in cooperation with all stakeholders a global culture of cyber-security,

*recognizing*

a) UNGA Resolutions 55/63 and 56/121 on "*Combatting the criminal misuse of information technologies*" and regional initiatives including, but not limited to, the Council of Europe's *Convention on Cybercrime*;

b) the outcomes of the two phases of the World Summit on Information Society, and especially, paragraphs 39 to 46 of the Tunis Agenda for the Information Society;

c) that paragraph 42 of the Tunis Agenda in particular affirmed "*that measures undertaken to ensure Internet stability and security, to fight cybercrime and to counter spam, must protect and respect the provisions for privacy and freedom of expression as contained in the relevant parts of the Universal Declaration of Human Rights and the Geneva Declaration of Principles.* »

d) that the Tunis Agenda for the Information Society has in addition identified ITU as a possible facilitator/moderator for action C5 on "Building confidence and security in the use of ICTs",

*aware*

a) that the global interconnection of telecommunication networks requires increased cooperation among governments, the private sector and civil society in respect of these systems and networks, in particular with the users interests in mind;

b) that ITU and other international bodies and organizations, through a variety of activities, are examining issues related to telecommunication network security, including network security and stability and measures to combat spam, malware, and illicit content as well as to protect personal data and privacy;

c) that the Tunis Agenda paragraph 41, mirroring WTSA 2004 Resolution 51 on "Combating Spam", recommended to counter such threats through "a multi-pronged approach [...] that includes, inter alia, consumer and business education; appropriate

Formatted: Bullets and Numbering

Deleted: that the application and development of ICT has been instrumental in the growth and development of the global economy,¶

Deleted: information and communication

Deleted: and

Deleted: information and communication

Formatted: Font: Italic

legislation, law enforcement authorities and tools; the continued development of technical and self-regulatory measures; best practices; and international cooperation”;

*d)* that the General Secretariat of the ITU and the sectors have already organized several workshops on cybersecurity, spam and other security issues;

Formatted: Font: Italic

*e)* that Study Group 17 of the ITU Telecommunication Standardization Sector and other ITU-T study groups are studying these issues;

Deleted: c)

*f)* that the World Telecommunication Development Conference of Doha has adopted the Action Plan of Doha and its programme 3 on “e-strategies and ICTs applications” that identifies cybersecurity as a priority activity of BDT and defines activities to be undertaken by the BDT, noting

Deleted: working on information and communication network security

Deleted: ,

Formatted: No underline, Font color: Auto, German (Germany)

a) that, as an intergovernmental organization with participation by the private sector, ITU is positioned to help to address threats and vulnerabilities, as they affect telecommunication networks, and therefore should play a key role in this regard;

Deleted: ¶

Formatted: German (Germany)

b) that ITU should build on its technical expertise in discussions on network security,

Deleted: information and communication network security

Deleted: n active

*c)* that other relevant international and regional organizations, such as the IETF, ISO, OECD, EU or APEC, as well as the private sector, are also working on these issues.

Deleted: information and communication

Formatted: Font: 12 pt, Italic

Formatted: Font: 12 pt

*resolves*

to strengthen the role of ITU in enhancing security and stability, by addressing threats and vulnerabilities of ICT networks, in particular the issue of countering spam,

Deleted: information and communication network

*instructs the Secretary-General and the Directors of the Bureaux*

1 to review, on the basis of a status report on work done so far by ITU and other relevant organizations, ITU's current activities in network security and stability, by addressing existing and future threats and vulnerabilities of ICT networks, in particular the issue of countering spam, in liaison with other relevant international and regional organizations and initiatives, for example the IETF, the APEC Anti-Spam Strategy, the London Action Plan, the Seoul-Melbourne Anti-Spam Memorandum of Understanding and the relevant activities of OECD;

Deleted: ITU's current activities in information and communication network security

2 to intensify work within existing ITU study groups in order to:

i) reach a common understanding on the importance of network security and stability by addressing existing and future threats and vulnerabilities of ICT networks, by studying technologies, products and services, in order to develop recommendations, as appropriate;

Deleted: of information and communication network security

Deleted: standards on

Deleted: with a view

ii) seek ways to enhance the exchange of technical information in these fields, promote implementation of emerging protocols and standards that further enhance security and promote international cooperation among appropriate entities;

Deleted: ing

Deleted: of information and communication network security, and

iii) report on the result of these studies annually to the ITU Council,

*invites ITU Member States and Sector Members*

to participate actively in the ongoing activities and in the work of the relevant ITU study groups.