INTERNATIONAL TELECOMMUNICATION UNION

TELECOMMUNICATION STANDARDIZATION SECTOR

STUDY PERIOD 2009-2012

COM 17 – LS 006 – E

English only

Original: English

Question(s):	4/17	Geneva, 11-20 February 2009

Ref. : TD 0244 Rev.2

Source:	ITU-T SG 17 (Geneva, 11-20 February 2009)
Title:	Collaboration in the work on global cybersecurity

LIAISON STATEMENT

For action to:	ITU-T SG 13 Q.16/13; ITU-T SG 16 Q.17/16; ITU-T SG 2; OMA; WSIS; ETSI TC GRID; ETSI TC LI; ETSI TISPAN; ETSI ESI; ISO/IEC JTC 1/SC 27/WG 4; IEEE; IETF; ICANN; OASIS; 3GPP; 3GPP2; OECD; FIRST; CERT/CC; CSIRTs; ASCLAD; HTCIA; CAB Forum; Interpol; CNCERT/CC; Malaysia; Australia; International Organization on Computer Evidence (IOCE); US Dept of State; US GTISC; US Cylab/CERT; US MITRE; Public Safety Canada; ENISA; UK CPNI; UK CESG; France, Ministère de l'Intérieur, SGDN; Kapersky Labs; iDefense
For comment to:	
For information to:	
Approval:	**Agreed to at SG 17 meeting**
Deadline:	**1 June 2009**

Contact:	Tony Rutkowski Rapporteur, Q.4/17	Tel: +1-240-373-4056 Email: trutkowski@netmagic.com
Contact	Arkadiy Kremer Chairman, SG 17	Tel: +7 495 673 3246 Email: kremer@rans.ru

The Telecommunications Standardization Sector of the International Telecommunication Union (ITU-T) at its World Telecommunication Standardization Assembly (WTSA) in late 2008 designated cybersecurity and related infrastructure as a substantial challenge and priority for technical cooperative work for all its constituent nations and the telecommunication/ICT industry. WTSA-08 created within Study Group 17 on security, a Question for Cybersecurity designated Q.4/17.

At its first meeting since WTSA-08, the Cybersecurity Question adopted a focussed action plan that includes outreach and collaboration with a broad array of organizations that are significant venues in addressing cybersecurity and infrastructure protection. One of the most basic needs is simply identifying and effecting lines of communication among all these organizations. The needs are especially significant for countries that lack the resources to participate in the many forums, yet are part of the global network cybersecurity and vulnerability mosaic.

Attention: Some or all of the material attached to this liaison statement may be subject to ITU copyright. In such a case this will be indicated in the individual document.
Such a copyright does not prevent the use of the material for its intended purpose, but it prevents the reproduction of all or part of it in a publication without the authorization of ITU.

Through this liaison communication, we are reaching out to you to be part of this global effort and share aspects about what is occurring in our respective organizations, and collaborating to the extent you have resources and interests in global cybersecurity. We are providing information from our initial action plan and will follow-up with further communications. Over the coming weeks, a reply to this communication is appreciated. Please send your replies to:

Mr. Georges Sebek
Counsellor for ITU-T SG 17
ITU/TSB
Place des Nations
CH-1211 Geneva 20
Switzerland
Tel: +41 22 730 5994
Fax: +41 22 730 5853
E-mail: tsbsg17@itu.int

Attachment: **1**

Adapted from Q.4/17 (Cybersecurity) action plan

ATTACHMENT to COM 17-LS 0006

Adapted from Q.4/17 (Cybersecurity) action plan

1 Motivation

The cybersecurity landscape is constantly changing. Currently there is a strong need for securing the cyber environment for protocols, infrastructures, applications such as those providing voice, multi-media, information assurance, identity and data services, for conducting business, providing emergency based services, social networking and as the medium for connecting people and services.

Cybersecurity involves more than securing the critical infrastructure. It involves securing and protecting services and personally identifiable information, protecting privacy, and providing information assurance (IA) among interacting entities.

Cyber attacks have become a widespread, global and borderless problem causing a complex range of problems to users, service providers, operators and networks. Tracing cyber attacks by technical means requires development of framework and requirements for detecting, protecting against, mitigating the effects of and recovering from cyber attacks, and covering important technical issues facing network operators, enterprises, and governments. ITU-T can help to make the cyber-world a safer place by investigating the technologies for tracing cyber attacks.

In light of these rapidly emerging developments, it was also considered critical to the World Telecommunication Standardization Assembly held in Johannesburg (October 2008) that *Cybersecurity*, subject of WTSA-08 Resolution 50 be given high attention given the crucial importance of the information and communication technologies (ICT) infrastructure to practically all forms of social and economic activity. Another WTSA-08 Resolution included facilitation to the newly emerging national Computer Incident Response Teams (CIRTs) recognizing the increasing attacks and threat on ICT networks through computers.

These actions also complemented cybersecurity related initiatives undertaken by other ITU organs in the development (ITU-D) and radio (ITU-R) sectors, as well as the General Secretariat. For example, the global nature of the challenges faced in making the information society safer and more secure resulted in discussions and agreements during the World Summit on the Information Society (WSIS) which looked to the ITU to facilitate the coordination of a global response to building confidence and security in the use of ICTs. In response to this role, ITU Secretary-General launched the Global Cybersecurity Agenda (GCA) as a framework for international cooperation with the objectives of leveraging existing initiatives and forging the necessary partnerships and alliances for a coordinated harmonized and global response.

Resource constraints

Cybersecurity is a broad problem domain, encompassing variety of threats and problem-solving techniques. Ideally, it is hoped to achieve maximum coverage in this domain by delivering a set of standards that cover every kind of threat and problem-solving techniques. It is not realistic however, due to resource constraints in participating organizations.

Typical strategy under the resource constraints would be to cover most of threats efficiently by finding a small number of cross-cutting concerns, or attributes. In the past, similar effort in standardization bodies resulted in well-known attributes of confidentiality, integrity, availability and authenticity. Among the proposed new work items, traceability and forensic capability might be new attributes that can be brought into future ICT infrastructure.

Threat-based modeling, such as spam, botnet detection and traffic anomaly detection, should also attempt to 1) find cross-cutting concerns among several threats, and 2) reuse the deliverables of

attribute-based work items; we should avoid duplication of efforts among threat-based work items. For example, some operational aspects of spam and botnet mitigation activities can be addressed by a security information sharing framework, which is a cross-cutting concern.

Standardization based on experiences

Good international standardization is supported by experiments and operational experiences within one or more member countries. This is particularly important, since there are a large diversity of established practices among countries. According to a variety of global statistics, some countries are ahead of others in overall cybersecurity today.

Gap analysis and resource assignment

Q.4/17, as part of all its work, should conduct a gap analysis of existing practices and its own agenda. It should be possible to identify a set of cybersecurity practices that significantly improve the measurable state of cybersecurity. The gap analysis will help prioritize a set of work items not only for Q.4/17 work, but also, where applicable, help guide resource assignment within each country.

2 Objectives

Serve as the lead Rapporteur group for treating the following questions:

a) How should telecommunication network providers secure and protect their infrastructure, maintain secure operations and use security assurance mechanisms in telecommunication networks?

b) What are the security requirements that software, telecommunication protocols, communication systems designers and manufacturers need to consider in the design, development and sharing of best practices in the cyber environment?

c) How should vulnerabilities information be shared efficiently to aid in vulnerability life-cycle processes?

d) What requirements and solutions are needed for telecommunications/ICT digital forensics, trace-back, and abnormal traffic detection?

e) What framework for security information and security policy sharing is needed?

f) What are the necessary guidelines and best practices that should be considered by telecommunication/ICT service providers?

g) Assist in the elaboration of global standards and procedures for the establishment and coordination of national CIRTs in application of WTSA-08 Resolution 58, *Encourage the creation of national computer incident response teams, particularly for developing countries*.

h) How can networks be used to provide critical services in a secure fashion during national emergency?

i) What enhancements to existing Recommendations under review or new Recommendations under development should be adopted to reduce impact on climate changes (e.g., energy savings, reduction of green house gas emissions, implementation of monitoring systems, etc.) either directly or indirectly in telecommunication/ICT or in other industries?

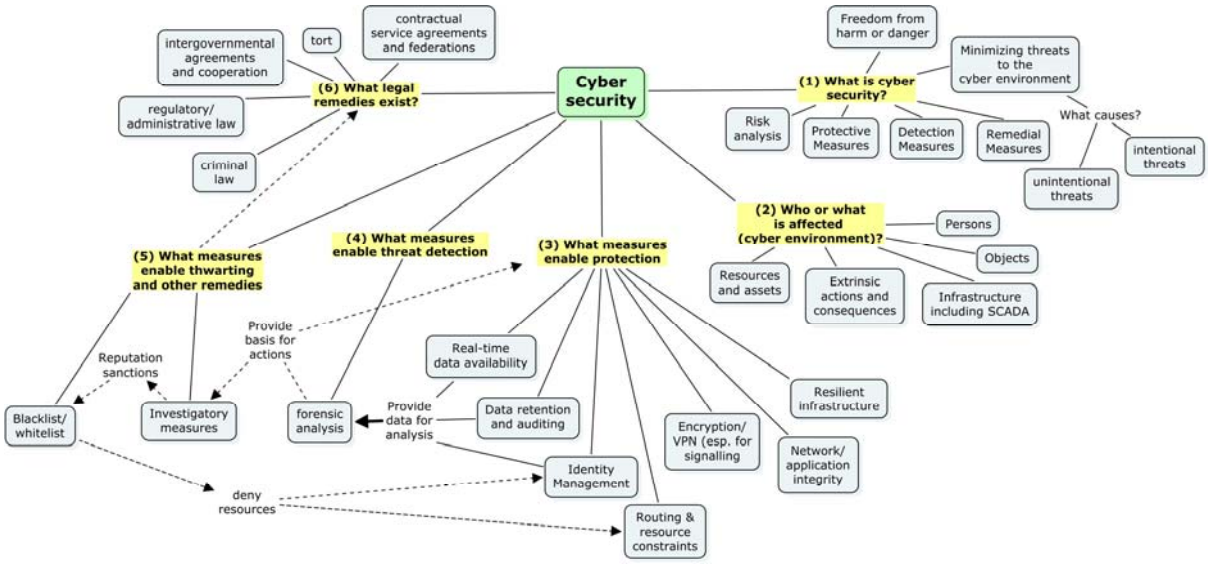

Fig. 1 – Global Cybersecurity Ontology

3 Tasks

Tasks include, but are not limited to:

a) Continue to develop a shared global cybersecurity ontology, building on and evolving Figure 1, above, and evolving related Recommendations, especially ITU-T X.1205. This will include a cybersecurity terminology reference recommendation.

b) Collaborate with a broad array of identifiable standardization bodies and forums on cybersecurity, including CERTs/CIRTS, using all available technologies, including liaisons, outreach activities, a cybersecurity developments exchange list, a website/wiki for organizations and activities, and a global cybersecurity calendar.

c) Assisting in the development of the ITU-D Framework for Organizing a National Approach to Cybersecurity and its 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.

d) Collaborate with Next Generation Networks activities in ITU-T in the areas of Cybersecurity.

e) Identify and develop standards required for addressing the challenges in Cybersecurity, within the scope of Q.4/17.

f) Work on frameworks for secure network operations to address how telecommunication/ICT network providers protect their infrastructure and maintain secure operations.

g) Produce a set of Recommendations for providing security solutions for telecommunication/ICT forensics and their trusted sharing globally.

h) Work on security assurance mechanisms and associated risk assessment and management in telecommunication/ICT networks.

i) Work on means for the exchange of information in networks in a secure fashion. This includes collaborating with Q.10/17 (Identity management architecture and mechanisms) in their study of authentication assurance, level of trust in the exchanged information, level of trust in authenticated devices and authenticated users.

j) Study and specify the techniques and capabilities for network and service providers to coordinate and exchange information regarding network forensics and cyber attacks.

k) Develop best practices and guidelines for the sharing of vulnerabilities information and updates and patches to aid in the vulnerability life-cycle processes.

l) Study and consider how to best use trace-back mechanisms in the telecommunication/ICT networks.

m) Study and develop the requirements for safe software programs that can effectively deal with rogue programs like spam, virus etc.

n) Provision, availability and use of critical services in a secure fashion during national emergencies, especially as it relates to ITU-T X.1303 (CAP).

o) Maintain awareness of the implications of regulatory requirements for telecommunications from a cybersecurity perspective, especially those relating to ITU treaty instruments.

p) Develop guidelines and techniques for the implementation of trusted provider identities for cybersecurity purposes.

q) Protection of personally identifiable information (PII).

r) Provide assistance and outreach to other ITU-T study groups and, as appropriate, the cybersecurity community in applying relevant cybersecurity solutions – especially in developing countries.

s) Review project-oriented security solutions for consistency.

4. Work programme

a) Recommendations approved:

- 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.1303, Common alerting protocol (CAP 1.1)

b) Recommendations under development:

- Draft ITU-T X.abnot, Abnormal traffic detection and control guideline for telecommunication network

- Draft ITU-T X.bots, Frameworks for botnet detection and response

- Draft ITU-T X.dexf, Digital evidence exchange file format

- Draft ITU-T X.gopw, Guideline on preventing malicious code spreading in a data communication network

- Draft ITU-T X.gpn, Mechanism and procedure for distributing policies for network security

- Draft ITU-T X.sips, Framework for countering cyber attacks in SIP-based services

- Draft ITU-T X.sisfreq, Requirements for security information sharing framework

- Draft ITU-T X.tb-ucc, Traceback use case and capabilities

_____