ITU Global Cybersecurity Agenda (GCA)

High-Level Experts Group (HLEG)

REPORT OF THE CHAIRMAN OF HLEG

To ITU Secretary-General,

Dr. Hamadoun I. Touré

by

Chief Judge Stein Schjølberg,

Judge at the Moss Tingrett Court, Norway

---

1 INTRODUCTION

In response to its mandate as sole Facilitator of WSIS Action Line C5, the ITU Secretary-General, Dr. Hamadoun I. Touré, launched the Global Cybersecurity Agenda (GCA) on 17 May 2007 as a framework for international cooperation to promote cybersecurity and enhance confidence and security in the information society. The GCA seeks to encourage collaboration amongst all relevant partners in building confidence and security in the use of Information and Communication Technologies (ICTs).

The GCA has benefited from the advice of an expert panel, the High-Level Experts Group (HLEG), on the complex issues surrounding cybersecurity. The HLEG is a group of specialists in cybersecurity, comprising more than one hundred experts from a broad range of backgrounds in policy-making, government, academia and the private sector. This Report is the final Report from the Chairman of the HLEG to the Secretary-General of the ITU, Dr. Hamadoun I. Touré, for his consideration. It has been drafted on the basis of the deliberations of the HLEG.

I should like to extend my sincere thanks to the Work Area leaders and all HLEG Members for their active participation and superlative contributions, which have helped make the collaborative efforts of the HLEG a success and have made this Report possible.

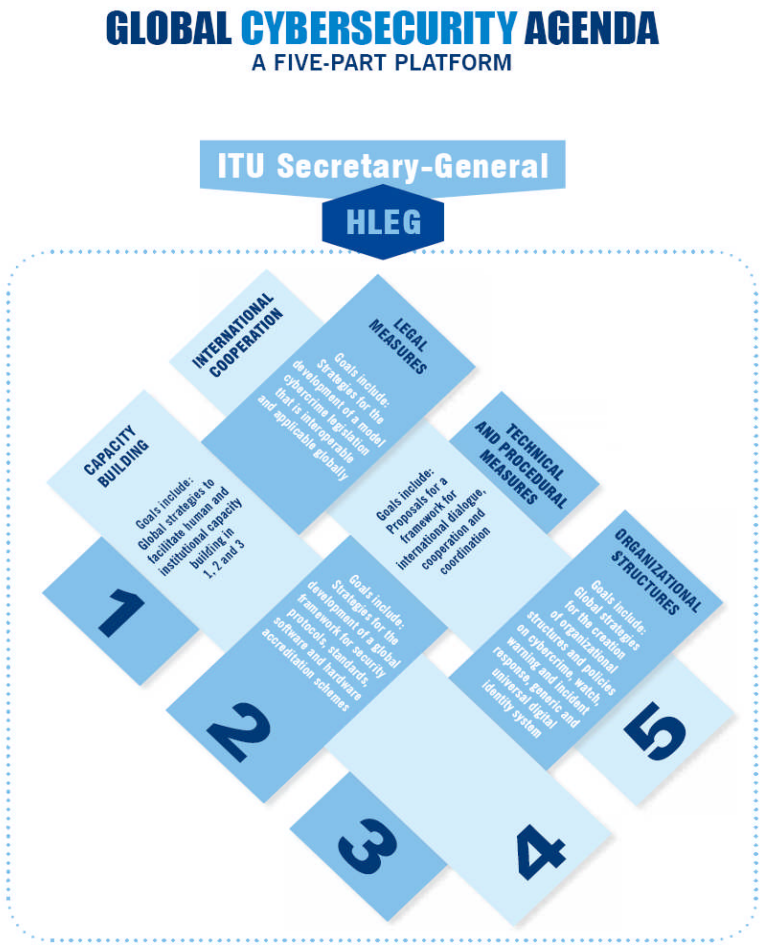
2 THE GLOBAL CYBERSECURITY AGENDA (GCA)

Cybersecurity is one of the most profound challenges of our time. The rapid growth of ICT networks has created new opportunities for criminals to exploit online vulnerabilities and attack countries' critical infrastructure. Governments, firms and individuals are increasingly reliant on the information stored and transmitted over advanced communication networks. The costs associated with cyberattacks are significant – in terms of lost revenue, loss of sensitive data, damage to equipment, denial-of-service attacks and network outages. The future growth and potential of the online information society are in danger from growing cyberthreats. Furthermore, cyberspace is borderless: cyberattacks can inflict immeasurable damage in different countries in a matter of minutes. Cyberthreats are a global problem and they need a global solution, involving all stakeholders.

At the World Summit on the Information Society (WSIS), government leaders recognized the real and significant risks posed by cybercrime and entrusted the ITU to take the leading role in coordinating international efforts on cybersecurity, as sole Moderator/Facilitator of WSIS Action Line C5, "Building confidence and security in the use of ICTs".

In response to this mandate, the ITU Secretary-General, Dr. Hamadoun I. Touré, launched the Global Cybersecurity Agenda on 17 May 2007 as a framework for international cooperation aimed at proposing strategies for solutions to enhance confidence and security in the information society. It seeks to build on existing national and regional initiatives to avoid duplication of work and encourage collaboration amongst all relevant partners. The GCA is built upon five key Work Areas:

Work Area one, "Legal measures", sought to develop advice on how criminal activities committed over ICTs could be dealt with through legislation in an internationally compatible manner. Work Area two, "Technical and procedural measures", focused on key measures for addressing vulnerabilities in software products, including accreditation schemes, protocols and standards. Work Area three, "Organizational structures", considered generic frameworks and response strategies for the prevention, detection, response to and crisis management of cyberattacks, including the protection of countries' critical information infrastructure systems. Work Area four, "Capacity building", sought to elaborate strategies for capacity-building mechanisms to raise awareness, transfer know-how and boost cybersecurity on the national policy agenda. Finally, Work Area five, "International cooperation" sought to develop a strategy for international cooperation, dialogue and coordination in dealing with cyberthreats.



3 THE HIGH-LEVEL EXPERTS GROUP (HLEG)

An expert panel was appointed to advise the ITU Secretary-General on the complex issues surrounding cybersecurity, consisting of world-renowned specialists in the subject. Members of the High-Level Experts Group (HLEG)[1] were nominated by the ITU Secretary-General, with due consideration to both geographical diversity and range of expertise, to ensure multi-stakeholder representation. It comprised more than one hundred world-renowned specialists in cybersecurity, representing expertise from across a broad range of backgrounds including the administrations of ITU Member States, industry, regional and international organizations, research and academic institutions.

3.1. Main Responsibilities of the HLEG

The key purpose of the HLEG was to advise the ITU Secretary-General on the complex issues surrounding cybersecurity and to formulate proposals on long-term strategies to promote cybersecurity in the five key Work Areas. The main responsibilities of the HLEG were:

- to further develop GCA by proposing refinements to its main goals;
- to analyze current developments in cybersecurity, including both threats and state-of-the-art solutions, anticipate emerging and future challenges, identify strategic options, and formulate proposals to the ITU Secretary-General;
- To meet the goals of GCA; and

[1] Details and biographies of HLEG Members are listed at: http://www.itu.int/osg/csd/cybersecurity/gca/hleg/members.html

- To provide guidance on possible long-term strategies and emerging trends in cybersecurity.

HLEG Members acted in their personal capacity and at their own expense, so their advice can be considered as objective and impartial. To ensure a representative balance in the membership of the HLEG, its members were nominated as a broad cross-selection from Member States from the five world regions; industry (manufacturers, operators, service providers, software developers, security and other information technology firms) and other regional and international organizations, academic and research institutions.

3.2. Structure and Working Methods

A collaborative portal was established, providing web-based electronic services for the submission and exchange of documents and allowing online real-time discussions between HLEG members. A Discussion Forum was created, allowing HLEG members to exchange views and ideas on all five Work Areas, follow discussion threads and respond to specific items that had been posted. A Wiki area was established, enabling HLEG members to post and upload resources, links and articles on cybersecurity and the different Work Areas of the GCA. A Documents area was created for HLEG members to upload written contributions and the outcome documents resulting from the work of the GCA. There was also a Chat area, enabling members to engage in on-line discussion with other users who were logged-on. The ITU Secretariat created an email account (gca@itu.int) which was used to contact the ITU Secretariat. Furthermore, a GCA mailing list was established to facilitate communications between HLEG Members through the direct exchange of emails.

At its Inaugural Meeting on 5 October 2007, the HLEG appointed Work Area leaders on a voluntary basis in order to deliver a strategic report in each of the five Work Areas:

1) Legal Measures: Mr. Stein Schjolberg, Judge at the Moss District Court, Norway.

2) Technical and Procedural Measures: Mr. Jaak Tepandi, Professor of Knowledge Based Systems, Institute of Informatics, Tallinn University of Technology, Estonia and Mr. Justin Rattner, Chief Technology Officer, Intel.

3) Organizational Structures: Mr. Taïeb Debbagh, Secretary-General, Département de la Poste, des Télécommunications et des Technologies de l'Information (DEPTTI), Kingdom of Morocco and Ms. Solange Ghernaouti-Helie, Professor and Présidente de la Commission Sociale, HEC-Université de Lausanne, Switzerland.

4) Capacity Building: Mr. Ivar Tallo, Senior Programme Officer, United Nations Institute for Training and Research (UNITAR) and Ms. Solange Ghernaouti-Helie, Professor and Présidente de la Commission Sociale, HEC-Université de Lausanne, Switzerland.

5) International Cooperation: Mr. Shamsul Jafni Shafie, Director, Security, Trust and Governance Department, Content, Consumer and Network Security Division, Malaysian Communications and Multimedia Commission and Mr. Zane Cleophas, Chief Director, Border Control Operational Coordinating Committee (BCOCC), Department of Home Affairs of South Africa.

3.3. HLEG Meetings

The HLEG held three official Meetings on 5 October 2007, 21 May 2008 and 26 June 2008, with a further two ad-hoc Meetings between the First and Second HLEG Meetings to supplement its work and activities (held on 7-8 January 2008 and 28-29 April 2008).

First HLEG Meeting:

The Inaugural Meeting of the HLEG took place at the ITU Headquarters in Geneva on 5 October 2007. At this meeting, HLEG members agreed on the strategy and work plan for their work. Members endorsed the five Work Areas and agreed on the expected deliverables of five strategic reports with a

set of recommendations, and a final consolidated report to be delivered to the ITU Secretary-General outlining strategies on how best to achieve the GCA's seven strategic goals.

Ad-hoc Meetings:

At the request of the leaders of the five Work Areas, two Ad-Hoc Meetings of the HLEG were held. At the First Ad-Hoc HLEG Meeting, held on 8-10 January, HLEG members reviewed and decided on a structure for their work in for each of the five Work Areas. HLEG members volunteered to collaborate in Work Areas of their expertise. At the Second Ad-Hoc HLEG Meeting, from 28-29 April 2008, leaders presented initial drafts of the strategic reports and agreed to revise the current versions of each strategic report, in light of the discussions between HLEG members. It was agreed that Work Area leaders would make the revised strategic reports available to all the HLEG Members on the collaborative platform from 12 May 2008. HLEG Members were encouraged to review the revised strategic reports and make suggestions until 19 May 2008.

Second HLEG Meeting:

The Second Meeting of the HLEG took place on 21 May 2008, with objectives of building on the momentum generated since the launch of the GCA and discussing the next steps for HLEG. Work Area leaders presented and discussed the draft strategic reports, as well as how to elaborate the recommendations arising from all five Work Areas, to be presented to ITU Secretary-General. During this meeting, it was agreed that:

- Work Area leaders would revise the strategic reports, in light of HLEG members' discussions;
- HLEG members were invited to send their comments on the draft recommendations.
- Strategic reports and recommendations were circulated to all HLEG members.

Third HLEG Meeting:

The Third Meeting of the HLEG took place on 26 June 2008 with the objective to agree on the set of recommendations to be presented to ITU Secretary-General in all five Work Areas. All five Work Area leaders presented draft recommendations for discussion and endorsement by HLEG members.

3.4. Outcomes of the HLEG

The lengthy, and often complex, deliberations of this panel of experts have achieved some important outcomes. The HLEG has proposed recommendations to the ITU Secretary-General on long-term strategies to combat cybercrime and promote Cybersecurity, based on a strategic report in each Work Area of the GCA. These recommendations are presented in the next section of this Report, Section 4, with an annotated summary of the views and discussions during the meeting relating to each Recommendation.

4 HLEG RECOMMENDATIONS

Cybersecurity is a complex issue with far-reaching consequences requiring close examination from a variety of different perspectives. Although HLEG members did not achieve full consensus in every recommendation, I am pleased to report that most of the HLEG experts were nevertheless in broad agreement on many recommendations that set a clear direction for ITU's future work in the domain of cybersecurity. In particular, HLEG Members were in full agreement that vital action is needed to promote cybersecurity and ITU has an important role to play. Recommendations were made in the following areas:

1) Legal Measures

Overview:

Work Area one (WA1) sought to promote cooperation and provide strategic advice to the ITU Secretary-General on legislative responses to address evolving legal issues in cybersecurity. Some HLEG members considered that the scope of WA1 included prosecution of cybercrimes. One member suggested the following summary of WA1: "ITU's Secretary-General should promote cooperation among the different actors so that effective legal instruments are identified and characterized in building confidence and security in the use of ICTs, making effective use of ITU recommendations and other standards, in accordance with present international agreements".

Summary of Discussions:

Discussions covered how to build on existing agreements in this area: for example, the Council of Europe's *Convention on Cybercrime* and the *Convention on the Prevention of Terrorism of 2005*. Some members preferred omitting mention of the *Convention on Cybercrime*, although they recognized it as an available reference. One member stated that the *Convention on Cybercrime* could not be proposed as the only solution for all states and wished to acknowledge the status of the *Convention* as an example of legal measures realized as a regional initiative belonging to signatory countries, consistent with the status accorded to the Convention in paragraph 40 of the WSIS Tunis Agenda for the Information Society.

There was considerable discussion as to whether recommendations 1.1-1.3 should be merged. Some members supported the suggestion that Recommendations 1.1-1.3 should be merged (e.g. some members wished to delete Recommendation 1.3). One key recommendation emerging from WA1 was that ITU could organize a global conference to promote cybersecurity, but this was contentious for some HLEG members (recommendation 1.13).

WA1 Recommendations:

1.1. ITU is a leading organisation of the UN system and could elaborate strategies for the development of model cybercrime legislation as guidelines that are globally applicable and interoperable with existing national and regional legislative measures.

1.2. Governments should cooperate 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 relevant initiatives including, but not limited to, the Council of Europe's *Convention on Cybercrime*.

1.3. "Considering the Council of Europe's *Convention on Cybercrime* as an example of legal measures realized as a regional initiative, countries should complete its ratification, or consider the possibility of acceding to the Convention of Cybercrime. Other countries should, or may want to, use the Convention as a guideline, or as a reference for developing their internal legislation, by implementing the standards and principles it contains, in accordance with their own legal system and practice.

With regard to the Council of Europe's Convention on Cybercrime, some members suggested that countries could be encouraged to join and ratify the Convention and draw on it in drafting their relevant legislation. One member suggested that countries could, or may want to, use the Convention as a guideline, or as a reference for developing their internal legislation, by implementing the standards and principles it contains, in accordance with their own legal system and practice. Other members preferred omitting mention of the Convention on Cybercrime, although they recognized it as an available reference, whilst one member stated that the Convention could not be proposed as the only solution for all states and wished to acknowledge that the Convention is an example of legal measures

realized as a regional initiative belonging to those countries which are signatories, consistent with the status accorded to the Convention in paragraph 40 of the WSIS Tunis Agenda for the Information Society. Some members wished to delete recommendation 1.3, despite the insertion of text recognizing the Convention as a regional initiative. One member wished to delete the phrase "may want to" in recommendation 1.3.

1.4. It is very important to implement at least Articles 2-9 in the substantive criminal law section, and to establish the procedural tools necessary to investigate and prosecute such crimes as described in Articles 14-22 in the section on procedural law.

A few members wished to delete this recommendation.

1.5. Cybercrime legislation should be designed using existing international and regional frameworks as a reference or as a guideline, and the Convention on Cybercrime was designed in a way so that it could be adapted to technological developments, and laws using the Convention as a guideline should be able to address modern developments.

One member wished to delete the first phrase on how cybercrime legislation should be developed. A few other members wished to delete the text referring to the history of the design of the Convention and the normative statement as to what it might be able to achieve.

1.6. Discussions about how to address criminal activities related to online games have just begun. Currently, most states seem to focus on extending the application of existing provisions, instead of developing a new legal framework for activities in virtual worlds. Depending on the status of cybercrime-related legislation, most offences should be covered this way; otherwise, countries should consider an appropriate approach to cover such offences.

One member wished to delete this Recommendation.

1.7. Supplementing Articles in the Convention may however be necessary. Countries should especially consider legislation efforts against spam, identity theft, criminalization of preparatory acts prior to attempted acts, and massive and coordinated cyber attacks against the operation of critical information infrastructure.

A few members wished to delete the first sentence referring to the need for supplementing Articles in the Convention.

1.8. Countries should consider how to address data espionage and steps to prevent pornography being made available to minors.

One member considered that the term "data espionage" is ambiguous, and should be defined properly, whilst another member wished to remove this term. Two members wished to delete this recommendation.

1.9. The introduction of new technologies always presents an initial challenge for law enforcement. For example, VoIP and other new technologies may be a challenge for law enforcement in the future. It is important that law enforcement, government, the VoIP industry and ICT community consider ways to work together to ensure that law enforcement has the tools it needs to protect the public from criminal activity.

1.9.a Given the responsibility of government authorities in protecting their consumers, special attention should be given to requirements enacted by government authorities that bear directly on the infrastructure-based and operational requirements imposed on those who provide and operate network infrastructures and services, or supply the equipment and software, or end-users. The concept of shared responsibilities and responsible partnership should be underscored in the development of legal measures on cybersecurity obligations in civil matters. A coordinated approach between all parties is

necessary to develop agreements, as well as provide civil remedies in the form of judicial orders for action or monetary compensation instituted by legal systems when harm occurs.

Two members wished to delete this recommendation. Some members wished to replace the specific references to VoIP with more general text recognizing that the introduction of a broad range of new technologies presents initial challenges for law enforcement. One member supported reference to "government, industry and ICT community", whilst another wished to make more general reference to "all relevant parties" [who] "should work together to ensure that law enforcement has the tools, resources and training needed". One member proposed the specific insertion of the additional text in 1.9(a).

1.10. The implementation of a data retention approach is one approach to avoid the difficulties of getting access to traffic data before they are deleted, and countries should carefully consider adopting such procedural legislation.

Two members wished to delete this recommendation. Another member proposed the alternative text: "the implementation of a data preservation approach has proven to be a key resource to law enforcement in investigations. Development of a balanced and reasonable data retention requirement should be carefully examined, taking into account expectations of privacy, security risks, etc., when considering adopting such procedural legislation".

1.11. In the fight against terrorist misuse of the Internet and related ICTs, countries should complete their ratification of the *Convention on the Prevention of Terrorism of 2005*. Other countries should, or may want to, use the Convention as a guideline, or as a reference for developing their internal legislation, by implementing the standards and principles it contains, in accordance with their own legal system and practice. Article 5 on public provocation to commit a terrorist offence, Article 6 on recruitment for terrorism, and Article 7 on training for terrorism are especially important. In addition, the *Convention on Cybercrime* has been studied with relation to terrorist misuse of the Internet and has been found to be important for defense against it.

One member wished to delete the last sentence.

1.12. 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 personal and illegal gains. With this in mind, it is critical that police work closely with 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 addressing the problem.

General consensus was achieved in respect of this recommendation.

1.13. There are several challenges facing prosecutors today in order to successfully prosecute cybercrime cases. These challenges include: 1) implementation of relevant cybercrime legislation; 2) understanding the technical evidence; 3) collecting evidence abroad; and 4) being able to extradite suspects located abroad. Thus, international coordination and cooperation are necessary in prosecuting cybercrime and require innovation by international organizations and governments, in order to meet this serious challenge. The *Convention on Cybercrime* Articles 23-25 address basic requirements for international cooperation in cybercrime cases.

One member wished to delete the last sentence, while several other members wished to extend the reference to the Articles mentioned, with the replacement of Article 25 with 35.

1.14. In conducting cybercrime investigation and prosecution, countries should ensure that their procedural elements include measures that preserve the fundamental rights to privacy and human rights, consistent with their obligations under international human rights law. Preventive measures, investigation, prosecution and trial must be based on the rule of law, and be under judicial control.

General consensus was achieved in respect of this recommendation.

1.15. The ITU, as the sole Facilitator for WSIS Action Line C5, should organize a global conference with the participation of [ITU Membership] for Members, regional and [international] organizations on cybersecurity and [relevant private organizations] in cybercrime. Participating organizations include, but are 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 Organization for Economic Cooperation and Development (OECD), The Commonwealth, European Union, Association of South East Asian Nations (ASEAN), NATO and the Shanghai Cooperation Organization (SCO).

Many members supported the recommendation of a global conference to promote cybersecurity, whilst other members wished to remove this recommendation – one member voiced its strong opposition to this. One member emphasized that ITU conferences should be open in its membership, especially to developing countries, whilst another underlined the importance of ITU remaining open to collaboration. Several members included reference to ITU's mandate as Facilitator for WSIS Action Line C5 and proposed insertions in square brackets refining the scope of the stakeholders involved.

2) Technical and Procedural Measures

Overview: Work Area two (WA2) focused on key measures for addressing vulnerabilities in software products, including accreditation schemes, protocols and standards. Discussions covered how to build on existing work in this area, including *inter alia*, the Common Criteria and the work of ITU-T and other standardization organizations. There was no consensus on recommendations proposing that ITU could explore possibilities for a globally-accepted ICT Security accreditation framework (recommendations 2.10 & 2.11).

Recommendations:

2.1. With regards to opportunities to enhance collaboration with existing cybersecurity work outside of ITU, the ITU should work with existing external centers of expertise to identify, promote and foster adoption of enhanced security procedures and technical measures.

2.2. ITU should take steps to facilitate it 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 – to enhance cybersecurity capabilities worldwide.

One member preferred to refer to ITU being "a" global centre of reference rather than "the" global centre for reference, whilst another member expressed its opposition to making this change.

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 CSIRTs to join the existing global and regional conferences and forums, in order to build capacity for improving state-of-the-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.

2.4. ITU should establish a long-term commitment to develop and refine Study Group 1/Question 22 efforts to identify and promote best practices related to national frameworks for managing cybersecurity and CIIP, as well as to establish regional workshops that help identify and share techniques for establishing and maintaining comprehensive cybersecurity programmes.

2.5. With regards to general activities for procedural measures, to promote more efficient approaches for improving security and risk management processes, any initiatives or recommendations in the field of technical measures must build upon the important work that has been done by the ITU on the development of best practices and standards for cybersecurity.

2.6. With regard to standards that are developed by other standardization organizations, ITU could act as a facilitator in promoting collaboration between different standardization organizations with a view to ensuring that new standards are developed in accordance with the principles of openness, interoperability and non-discrimination.

2.7. HLEG experts called for investigation, analysis, and selection, in cooperation with ITU-T, ISO, 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 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.

One member agreed with recommendation 2.7, but wished to draw attention to the tendency to overstate security issues related to applications with a lack of attention to issues related to services and infrastructures in the security approach in ITU-T Recommendation X.805.

2.8. 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.

2.9. ITU should develop model recommendations that can assist governments specifying organizational environments where the procedural measures proposed by ITU should be used.

One member wished to delete recommendations 2.8 and 2.9. Another member proposed the development of 'models' in 2.9, rather than 'recommendations', so it does not imply that an ITU 'recommendation' will be developed (although that may ultimately happen, depending on the topic and work in ITU-T & ITU-D).

2.10. With regards to general activities for technical measures, to establish a globally accepted evaluation framework for Common Criteria for ICT security to ensure minimum security criteria and accreditation for IT applications and systems (hardware, firmware and software), HLEG called for the investigation, analysis, and selection (in cooperation with ITU-T, ISO, IEC, and other relevant bodies) of ICT security standards and frameworks that can be components of a globally-accepted Common Criteria for ICT security evaluation framework. The systems to be investigated for Common Criteria evaluation include hardware systems, firmware systems, operating systems, office systems, browsers, e-mail software, document management (including archiving), network communications, instant messaging, peer-to-peer networking, social networking, anti-virus software, and others.

2.11. HLEG called for the development of model recommendations specifying application environments where IT products which have earned a Common Criteria certificate are advised. It is expected that these application environments are in both public sector organizations (including governmental institutions), as well as private sector organizations that are vital from the CIIP perspective.

There was no consensus on recommendations 2.10 & 2.11, proposing that ITU could explore possibilities for a globally-accepted ICT Security accreditation framework. One member stated its view that the Common Criteria is a limited agreement between governments, with only a small number of ITU member states as signatories and even fewer have certification labs. While its principles of mutual recognition are important, trying to apply Common Criteria requirements to ICTs – today used largely

by military organizations – may not yield positive results. Another member proposed alternative wording for recommendation 2.10: "Encourage countries to participate in the "Common Criteria" recognition agreement and other relevant similar initiatives to support minimal security criteria and accreditation schemes for IT applications and systems (hardware, firmware & software)". Two members wished to delete recommendations 2.10 & 2.11.

2.12. Internet: HLEG Members called for the investigation of ways to collaborate with private industry to enhance the security of public communication networks and ISPs - for example, Trusted Service Provider (SPID) initiative, DNSSEC, or systemic and economic incentives for security for protection of global telecommunications might be further examined and discussed. In collaboration with private industry, the ITU may examine the role of ISPs in blocking spam and other issues. Particular attention should be paid to investigating results of SG 13 - ITU-T's largest and most active standards body that addresses global information infrastructure, Internet protocol aspects and NGNs - that has engaged a broad, large cross-section of industry players and technical bodies.

One member proposed alternative wording of "particular attention should be paid to the work of ITU – T SG 13 and SG 17 in technical aspects of spam; NGNs, related aspects of IP-based technology, and other relevant work of the relevant ITU-T SGs. The focus should continue to engage a broad, large cross section of global industry players and technical bodies".

2.13. Digital identity management (DIM): HLEG members called for the investigation of technical aspects and interrelationships with other Work Areas. In particular, significant security work on Identity Management has occurred among the ITU-T security community through the Identity Management Global Standards Initiative (IdM-GSI), SG-13, and SG 17.

2.14. HLEG members called for a review of the current architecture of the telecommunication/ICT infrastructure, including the Internet, and define the institutional arrangements, and the responsibilities and relationships between the institutions, required to guarantee continuity of a stable and secure functioning of the DNS server system, as well as the ability to provide other trusted and interoperable global identity management capabilities that include discoverable and secure identifier resolver services, particularly with relation to the ITU OID DNS.

A few members wished to delete recommendation 2.14. One member in particular wished to delete reference to DNS on the basis that it is outside ITU's mandate to review the current architecture of the Internet or to define the responsibilities and relationships between institutional arrangements, especially involving the functioning of the DNS server system. One member suggested that references to DNS should be deleted and suggested alternative wording of: "Initiate a review of the current architecture of the telecommunication/ICT infrastructure, as well as the ability to provide other trusted and interoperable global identity management capabilities that include discoverable and secure identifier resolver services".

2.15. Emerging technologies: HLEG members called for consideration to be given to risks related to implementation of new technologies and infrastructures (for example, emerging risks from mass use of mobile devices and RFID in security critical applications or ambient intelligence environments).

One member suggested alternative wording for recommendation 2.15: "Emerging technologies: examine the role, if any, of the ITU-T SGs in considering new technologies and infrastructures (for example…)". Another member suggested that collaboration in analysis with SMEs could enable ITU to help ICT owner operators and governments to proactively manage the risks of emerging technologies.

2.16. Management system and personal certifications: HLEG members called for the selection and improvement of information security management system certification schemes, as well as personal information security certifications.

One member wished to delete recommendation 2.16. Another member understood rec. 2.16 to refer to information on security management systems, and identity management systems and

certification/compliance mechanisms for potential users. This member believed that many ICT markets operate well based on supplier declarations of compliance. The selection of systems and certification/compliance mechanisms is the user's decision - UN agencies should only undertake selection processes for their own procurement, and not select them for others.

3) Organizational Structures

Summary: General consensus was reached on the recommendations for WA3, with no oppositions voiced for removal of any of the recommendations. Discussions focused on a potential framework for the evaluation and assessment of cybersecurity readiness. One member proposed that the ITU could develop a "Cybersecurity Readiness Index" based on a proposed Organizational Structures Framework including:

- A national leader for coordination in cybersecurity or National Cybersecurity Council.
- A national CERT/CSIRT representing either a government's IT security infrastructure protection or a national focal point for coordination.

Another member suggested that it might not be possible for every member state to create a national cybersecurity council, as there were no simple solutions. Instead, ITU could develop an assessment framework to evaluate cybersecurity. Another member suggested that ITU-D's work might address some of these issues.

One member proposed that Secretary-General could consider establishing a new ITU-D programme on capacity-building and skills for cybersecurity and CIIP that could focus on:

- identifying best practices of existing programs and developing materials that respond to the needs of member states;
- enhancing information security programmes for ICTs;
- identifying cyber-risk assessment and risk management methods for ICTs;
- developing and maintaining information regarding computer security incident response teams and capabilities for addressing changing threats in ICTs, especially in close collaboration with FIRST and other expert organizations.
- identifying methods to support emergency preparedness and continuity planning.
- The proposed programme could deliver regional workshops, skills enhancement seminars and conferences.

One member further suggested that the recommendations on organizational structures should be scalable and adaptable to different actors, promoting inclusion at the international level. Another member also suggested that member countries could:

- Take into account the recommendations issued from the ISO/IEC 27000-family information security standards on Information Security Management Systems to protect the confidentiality, integrity and availability of digital information and information systems.
- Develop and adopt national cybersecurity policies and strategies, and to mobilize the required resources for implementing them, with the support of the relevant stakeholders including government, private sector, academia and civil society.

One member called for greater recognition to be given to the ongoing work of ITU-D and Q22/1, although another member suggested that Q22/1 work might not always be scalable to all countries.

Recommendations:

3.1. ITU should provide assistance to developing and least developed countries in the elaboration and promotion of national policies in cybersecurity.

3.2. ITU should provide assistance to developing and least developed countries in the elaboration of national, regional and international strategies to fight against cybersecurity incidents in a global perspective;

3.3. ITU should assist governments in putting in place policies and strategies aimed at improving the coordination of cybersecurity initiatives at the national, regional and international levels;

3.4. ITU should assist countries in setting up organizational structures aimed at responding to the specific needs of countries, taking into account resource availability, public-private partnerships, and the level of ICT development in each country within the spirit of multi-stakeholder cooperation, as outlined in WSIS outcomes.

One member suggested that there should be greater mention of civil society. The role of civil society is very important, especially the WSIS multi-stakeholder approach.

3.5. ITU should encourage each country to develop its own strategy and organizational structures to address its national cybersecurity needs and should promote assistance through regional and international cooperation.

3.6. Taking into account the broad nature of issues to be addressed in cybersecurity and the characteristics of cybersecurity as outlined in the work of ITU-T SG 17, ITU should support countries in establishing appropriate organizational structures and capacity-building programmes.

One member suggested that the recommendations should take into account that the broadness of the cybersecurity issue (given the definition adopted by ITU-T SG 17) and may require different organizational structures, depending on the specific cybersecurity issue being addressed.

4) Capacity Building

Summary: General consensus was achieved on the recommendations in WA4. One member suggested the inclusion of additional recommendations:

- That the Secretary-General continue to support the work of ITU-D's regional cybersecurity conferences that bring together key SMEs from public and private sector organizations to address critical challenges related to cyber security/CIIP.
- That the Secretary-General advocate for enhancing computer science and telecommunications engineering curricula to ensure that it actually includes security as part of the core focus of study.

One member suggested that recommendations should be made clearer, by drawing on more specific substance in direct relation to the other Work Areas, while another member suggested that the recommendations should be more specific with regards to which skills and which efforts are needed. One member recommended using templates matching the various choices of organizational structures (at the national to regional to international level) and then identifying the different possible skills from the administrative level upwards to achieve strategic goals.

One member noted that the strategic report focuses on four layers, which have been divided as: end user, national, regional and international. Another member suggested that "regional" and "international" be integrated as "international". For each layer, the report should address what constitutes the improvement of capacity, who is the main actors, and what are the main activities and their expected outcomes. This member also noted that capacity-building for an inclusive society is

cross-cutting across the other four Work Areas of GCA and should be put in other 4 areas. Capacity building is just one part of building an inclusive society.

Recommendations:

4.1. ITU should 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.

One member proposed alternative text of: "ITU's lead role in coordinating robust, multi-stakeholder participation in cybersecurity investigation and solutions development and put them into action, develop effective legal framework in elaboration of strategies for the development of a model cybercrime legislation as a guideline that is globally applicable and interoperable with existing national and regional legislative measures in order to answer the needs identified in WA1". Another member suggested that the work of international bodies like the ITU who could play a role should be highlighted.

4.2. ITU should promote the adoption and 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.

One member proposed alternative text of: "Promote the adoption and the support of technical and procedural cybersecurity measures through four strategic proposals for the Secretary-General 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 topics,as specified by WA 2".

4.3. ITU should support ITU 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.

One member proposed alternative text of: "Support ITU members in development and promotion of national, regional and international policy and strategies to fight against cybersecurity incidents in a global perspective, including an improvement national, regional and international level governments coordination in cybersecurity; in graduated response, to organizational structures and capacity building needs bearing in mind local factors; put in place organizational structures as presented in WA 3".

4.4. ITU should create a focal point within the ITU to manage the diverse activities in a coordinated manner in order to support national, regional, international cooperation as defined by Work Area 5;

One member proposed alternative text of: "Create a focal point within the ITU to manage the diverse activities in a coordinated manner in order to support national, regional, international cooperation as defined by WA 5".

4.5. ITU should assist in empowering end-users to adopt a safe behaviour in order to become responsible cyber-citizens.

4.6. ITU should encourage providers of ICT products and services to increase the security of their products and services and to take steps to support end-users' cybersecurity measures;

4.7. ITU should train and educate at several levels all the actors of the information society;

4.8. ITU should continue to develop human capacity in all aspects of cybersecurity to help build a global culture of cybersecurity.

One member was concerned about how recommendation 4.8 relates to capacity-building – need actions to support the global framework, so it suggested alternative text: "Continue to develop human capacity in all aspects of cybersecurity to help build a global culture of cybersecurity".

4.9. ITU should 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.

4.10. ITU should make full use of NGOs, institutions, banks, ISPs, libraries, local trade organizations, community centres, computer stores, community colleges and adult education programmes, schools and parents-teacher organizations to get the cybersecurity message across.

4.11. ITU should promote awareness campaigns through initiatives for greater publicity.

5) International Cooperation

Summary: General consensus was achieved on the recommendations for WA5, with no opposition voiced. One member emphasized that there should be coordination with other Work Areas, including extension of the GCA mandate, supported by ITU in pragmatic ways.

Recommendations:

5.1. ITU should create a focal point within ITU to manage the diverse activities in a coordinated manner in order to ensure successful execution of the ITU mandate. The focal point would serve to ensure continuity in the ITU after the HLEG has completed its work, 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 and, as appropriate, develop compatible unified strategies and solutions. The functions of the structural focal point would include:

- To compile information on initiatives and activities in the field of cybersecurity and make this information available to all stakeholders
- 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 the 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).

- In accordance with the ITU's WSIS C5 mandate, to support and promote the work of other organizations who have expertise in cybersecurity areas in which the 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.
- To the extent they are within the ITU's mandate, to implement any HLEG recommendations that are approved by Council, without duplicating the work of other organizations in this area.
- To work with the global community on 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.
- To facilitate the coordination of the ITU's work in this field with other organizations to avoid duplication of effort and, to the extent possible, to assist in identifying and achieving compatible goals amongst the various individual initiatives.
- Work towards international harmonization of the activities of stakeholders in the various fields of cybersecurity.
- Act as an expert resource for assisting stakeholders in the resolution of international issues that might arise relating to cybersecurity.

It is recommended that the Secretary-General initiate a study to define more precisely the form and function of the proposed organization.

Two members queried the management of which & whose resources and activities. They suggested a clearer distinction should be made between ITU managing its resources, external bodies managing their resources and coordination between different bodies on their respective resources. One member called for policy coherence and coordination to avoid duplication of efforts.

Another member expressed appreciation that their comments on a focal point were taken into consideration – other cross-cutting areas (WSIS implementation, emergency comms) have focal points. Another member agreed with the proposal to create an ITU focal point, but suggested that one might already exist. One member suggested that a focal point already exists in ITU-D, which could be enhanced. Another member believed that the ITU needs to have more flexibility in this area and should not be limited to its mandate.

One member stated that ITU's mandate is defined by its Constitution and Convention and by WSIS C5. The only HLEG proposals that the focal point can implement are those within the ITU's mandate as set forth in these documents. This member noted that the WSIS outcome documents state that the role of the ITU is as a facilitator or moderator of Action Line C5. "Facilitate" means to "make easier." "Moderate" means "to preside over". They do not mean "coordinate" or "manage" or "harmonize." All of these words imply that the ITU is placing itself in an oversight/ directive role with respect to other organizations, which it is clearly not authorized to do. It is also inappropriate, because although the ITU has expertise in some areas of cybersecurity, it has no expertise in many others. This member stated its view that "coordination' implies oversight/ direction and is outside the authority of ITU for the reasons expressed below. It stated its view that "harmonization" implies oversight/direction and exceeds the mandate of WSIS C5. This member suggested that ITU should not get involved in resolving cybersecurity issues that are beyond the scope of its expertise. It believed that this section is out-of-scope as written and needs to be substantially re-written along the lines of the member's proposed terms of reference for the focal point, which closely follow the contours of the ITU's mandate, or alternatively, deleted.

5.2. The second proposal involves general activities for the monitoring, coordination, harmonizing and advocating international cooperation:

a) Monitoring - "In order to improve the potentiality for different stakeholders to achieve better synergies through their own initiative, on an optimum cost for benefit basis, and taking in to consideration the current role the ITU plays and the resources at its disposal, it is suggested that the Secretary-General create within the ITU structure a mechanism to gather information about the various projects and initiatives in the field of cybersecurity and to disseminate such information as widely as possible, as an immediate measure. It is further recommended that this mechanism utilizes equally the currently available resources within ITU and the relationships ITU has built with groupings of stakeholders". At a minimum, ITU should be monitoring the different initiatives and projects related to cybersecurity by various organizations (international, national, private and third sector) as means of and a prelude to promoting cooperation. This does not require much effort in the form of resources and strictly speaking does not even require the consent of the organizations whose projects/initiatives that are being monitored though their cooperation is most desirable. Making this information available to stakeholders will encourage and enable them to coordinate their activities. In addition, that will help immensely the other Work Areas as these Work Areas rely to a large extent on multilateral coordination on specific initiatives.

b) Coordination - "Having considered the efficiencies that could be achieved by coordinating the various activities, initiatives and projects of different stakeholders in the cybersecurity field along with the potentiality for better utilization of resources and results, it is recommended that the Secretary-General explore the possibility of creating a network for coordinating such activities, initiatives and projects, through agreements or memoranda of understanding. Given that all stakeholders may not receive such an initiative positively, especially those who may perceive this as a dilution of their sovereignty, it is recommended that the initiative be started on a voluntary basis. When a critical mass of stakeholders subscribe to the initiative, others may feel more encouraged to join in." If the political will and resources are available, ITU should take the lead in coordinating the work of various organizations in order to avoid duplications. This could be done at different scales depending on the extent of control that ITU would and could exercise, the willingness of ITU to undertake that role, the ability to obtain the consent of other organizations and the availability of resources. *At the lowest level, it could be simply tracking activities of all organizations that have a mandate on cybersecurity and making stakeholders aware of them as proposed above*. At the highest level, ITU could actively coordinate and drive the individual initiatives towards a common programme. The beneficial effects of coordination on the other Work Areas, especially in capacity-building, cannot be stressed more.

c) Harmonizing - "Based on the recommendations of the other Work Areas particularly legal and procedural & technical Work Areas, it is evident that these measures need to be harmonized across borders to the maximum extent possible, if the potential benefits are to be derived. In fact lack of harmonization would result in diluting the affect of proposed strategies to an unacceptable extent. Thus it is recommended that the ITU should strongly consider a strategy to harmonies these activities relating to cybersecurity while addressing satisfactorily the issues of independence and sovereignty of nations and groupings". "Having considered the efficiencies that could be achieved by coordinating the various activities, initiatives and projects of different stakeholders in the cybersecurity field along with the potentiality for better utilization of resources and results, it is recommended that the Secretary General explore the possibility of creating a network for coordinating such activities, initiatives and projects, through agreements or memorandum of understanding. Given that all stakeholders may not receive such an initiative positively, especially those who may perceive this as a dilution of their sovereignty, it is recommended that the initiative be started on a voluntary basis. When a critical mass of stakeholders subscribe to the initiative, others may feel more encouraged to join in".

d) Advocacy - "As knowledge and awareness plays a key role in ensuring cybersecurity and as the ITU is a trusted source of knowledge the world over, it is recommended that the ITU undertake the lead role in advocacy on cybersecurity at a degree and on a scale in keeping with its organizational aspirations, commensurate with resources at its disposal and is deemed practicable under the current context of

international relationships". ITU, with its mandate from Member States and its position in the UN system, is ideally placed to play the role of advocate. Its voice is heard and followed, its suggestions respected and mostly complied with. Thus, in order to bring about a culture of cybersecurity, it is important that ITU undertakes the primary role in advocacy. Advocacy could be undertaken at various levels from international fora to country or even community level. Again, the magnitude of the work in this arena depends on the level of resources available, the scale of ownership the ITU wishes to exercise and the realities of international relations.

One member agreed with the sub-points on harmonization and international cooperation, but felt that coordination and, to some extent, monitoring is not in accordance with ITU's role.

One member wished to delete from 5.2.(a)"this does not require much effort in the form of resources and, strictly speaking, does not even require the consent of the organizations whose projects/initiatives that are being monitored though their cooperation is most desirable". The same member also wished to delete from 5.2.(b) "memoranda of understanding. Given that all stakeholders may not receive such an initiative positively, especially those who may perceive this as a dilution of their sovereignty".

One member wished to delete from 5.2.(b) the sentence "At the lowest level, it could be simply tracking activities of all organizations that have a mandate on cybersecurity and making stakeholders aware of them as proposed above", because it repeats the "Monitoring" section above.

The same member wished to replace bullet point 5.2.(b) with "Facilitating - Having considered the efficiencies that could be achieved by facilitating the various activities, initiatives and projects of different stakeholders in the cybersecurity field along with the potentiality for better utilization of resources and results, it is recommended that the Secretary-General explore the possibility of creating a network that is inclusive and open for facilitating such activities, initiatives and projects, through a variety of mechanisms that are mutually agreeable. It is recommended that the initiative be undertaken on a voluntary basis. When a critical mass of stakeholders subscribe to the initiative, others may feel more encouraged to join in. Harmonizing would bring the ITU into areas that are not within its mandate".

One member wished to delete the bullet point on Harmonizing because the ITU does not have the expertise to be harmonizing legal systems around the world, or for that matter any area outside its field of expertise, e.g. incident response activities. This member drew attention to the fact that the organizational aspirations of the ITU are constrained by its mandate. Another member also wished to delete the bullet point on Harmonizing altogether.

One member wished to insert at the end of 5.2.(d): "and within the areas of expertise" and wished to add after "mandate from Member States", "and consistent with its Constitution and Convention and with the facilitating role for WSIS". Another member wished to delete from 5.2.(d) "Its voice is heard and followed, its suggestions respected and mostly complied with".

5.3. 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:

5.3.1. To facilitate the ITU 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; and

5.3.2. To encourage greater attention, involvement, and resources devoted to global collaborative forums – especially ITU's own forums in the T, D and R Sectors – to advance and expand the development, availability and use of these capabilities.

One member expressed concern that the Secretariat becoming the focal point for cybersecurity in the ITU could result in a "top-down" plan for cybersecurity, which ITU-T and ITU-D will be expected to implement. The work in the ITU-T and ITU-D has until now been based on a "bottom-up" approach. For example, in the ITU-T, work is driven by company contributions which are based on marketplace and industry needs and not by a plan. Similarly, in the ITU-D, the work program has been following the best practices developed by Member States and Sector Members in Q22. These best practices have been distilled from the experience of countries and sector members that have already developed and are implementing national cybersecurity plans, and also represent a "bottom-up' approach. This bottom-up approach has proven to be very effective.

One member proposed alternative text of: "the ITU Secretary-General should initiate necessary activities, especially involving the many experts in the ITU sectors, combined with resources from all Bureaux and the many other cybersecurity related bodies, with a continuing focus on the leadership of the ITU-D in capacity-building initiatives and programmes focused on the developing countries".

One member wished to add recommendation: "The Secretary-General should establish a collaborative initiative, in cooperation and conjunction with leaders of the key organizations for cybersecurity including OECD, Forum of Incident Response Teams (FIRST), Software Assurance Forum for Excellence in Code, ISACA, ISC2, IMPACT, ICANN and other key organizations to convene a yearly summit that focuses on key cybersecurity issues. The proposed Summit should be a day and a half summit immediately preceding the WSIS C5 Action Line implementation meetings. Collaborating to convene a senior-level summit will catalyze focus towards achieving the goals of C5 Action Line".

5 ACKNOWLEDGEMENTS

During the year since its launch, the GCA has achieved some notable key successes, including endorsement by the WSIS stakeholder community during the 2008 WSIS Action Line C5 Meeting as a credible multi-stakeholder global framework for international cooperation in addressing the global challenges in cybersecurity. The GCA has strengthened ITU's role as sole Facilitator/Moderator in WSIS Action Line C5 and provides the framework within ITU for internal coordination of ITU's own activities in cybersecurity.

The work of the High-Level Experts Group was supported by the voluntary participation of and thought leadership of more than one hundred experts representing a wide range of players in cybersecurity, at their own cost. This work has resulted in strategies and recommendations for addressing the wide range of challenges relating to global cybersecurity. The output of the High-Level Experts Group is represented by the set of recommendations, views and deliberations presented in this Chair's Report and the five strategic reports to be issued in one overall publication. I am proud to have been a part of this key initiative by the ITU and am pleased to have been able to contribute to its important work and significant achievements.

I would like to thank ITU Secretary-General for giving me the opportunity to chair this illustrious Group and to contribute to the work of this important ITU initiative.

These achievements would not have been possible without the dedication and sacrifices of the Members of the HLEG and especially the Work Area Leaders. I should like to thank all those who contributed actively to the work of the HLEG and especially, Mr. Jaak Tepandi, Mr. Justin Rattner, Mr. Taïeb Debbagh, Ms. Solange Ghernaouti-Helie, Mr. Ivar Tallo, Mr. Shamsul Jafni Shafie and Mr. Zane Cleophas.

I would also like to thank the Focal Points for Cybersecurity from the Radiocommunications (BR), Telecommunication Standardization (TSB) and Development (BDT) Bureaus for their guidance and support.

Finally, I would like to thank the Corporate Strategy Division for providing the secretariat support for the GCA and for their outstanding assistance to the HLEG that made it possible to finish these reports and recommendations so rapidly.

_____

_____

Chief Judge Stein Schjølberg, Judge at the Moss Tingrett Court, Norway

Signed on this _____ of _____ , _____ in_____ ,

(DAY) (MONTH) (YEAR) (CITY)

_____ .

(COUNTRY)

Stein Schjolberg

DN: CN = Stein Schjolberg C = NO O = Moss tingrett OU = Chief Judge
Date: 2008.09.02 08: 55:31 +01'00'
Reason: I am the author of this document
Location: Moss, Norway

6 ANNEXES

6.1 Annex 1: Strategic Report on Legal Measures

6.2 Annex 2: Strategic Report on Technical and Procedural Measures

6.3 Annex 3: Strategic Report on Organizational Structures

6.4 Annex 4: Strategic Report on Capacity Building

6.5 Annex 5: Strategic Report on International Cooperation

6.6 Annex 6: Contributions from HLEG Members

6.7 Annex 7: Relevant ITU Resolutions

7 LIST OF ABBREVIATIONS AND ACRONYMS

APEC	Asia-Pacific Economic Cooperation
ASEAN	Association of South East Asian Nations
AU	African Union
CIIP	Critical Information Infrastructure Protection
DIM	Digital Identity Management
DNS	Domain Name System
EU	European Union
FIRST	Forum of Incident Response and Security Teams
GCA	Global Cybersecurity Agenda
HLEG	High-Level Experts Group
ICTs	Information and Communication Technologies
IdM-GSI	Identity Management Global Standards Initiative
ID	Identity
IEC	International Electrotechnical Commission
IMPACT	International Multi-stakeholder Partnership Against Cyber-Terrorism
ISO	International Organization for Standardization
ISPs	Internet Service Providers
ITU	International Telecommunication Union
NATO	North Atlantic Treaty Organization
NGOs	Non-Governmental Organizations
OAS	Organization of American States
OECD	Organisation for Economic Cooperation and Development
RFID	Radio-Frequency Identification
SCO	Shanghai Cooperation Organization
SG	Study Group
UNITAR	United Nations Institute for Training and Research
UNODC	United Nations Office for Drugs and Crime
WA	Work Area
WSIS	World Summit on the Information Society