world summit on the information society
Geneva 2003 - Tunis 2005

International Telecommunication Union

BUILDING THE INFORMATION SOCIETY

Facilitation Meeting for WSIS Action Line C5 : Building confidence and security in the use of ICTs

Document: C5 Report
16 May 2006
Original: English

Chairman's Report
"Partnerships for Global Cybersecurity"

Geneva, 15-16 May 2006, ITU Headquarters

Purpose of this Report

1. In response to the calls by the World Summit on the Information Society (WSIS)[1] for implementation and follow-up on *building confidence and security in the use of ICTs*, at the invitation of the ITU Secretary-General, Yoshio Utsumi[2], the first facilitation meeting for WSIS Action Line C5 was organized at ITU Headquarters in Geneva, Switzerland on 15-16 May 2006. The meeting was held in conjunction with World Telecommunication Day[3] which had the theme *Promoting Global Cybersecurity*[4]. This Chairman's Report summarizes the discussions throughout the two days and presents below a high-level overview of the sessions and speaker presentations.

Background

2. The World Summit on the Information Society (WSIS)[5] was held in two phases. The first phase took place in Geneva hosted by the Government of Switzerland from 10 to 12 December 2003, and the second phase took place in Tunis hosted by the Government of Tunisia, from 16 to 18 November 2005.

3. The WSIS outcome documents[6] emphasize that *building confidence and security in the use of ICTs* is a necessary pillar in building a global information society. More specifically, the WSIS Declaration of Principles[7] states that "strengthening the trust framework, including information security and network security, authentication, privacy and consumer protection, is a prerequisite for the development of the Information Society and for building confidence among users of ICTs". It further states that a "… global culture of cybersecurity needs to be actively promoted, developed and implemented in cooperation with all stakeholders and international expert bodies".

4. The agreed WSIS texts that relate to *building confidence and security in the use of ICTs* can be found in Chapter 5 in both the Geneva phase's Declaration of Principles[8] and Plan of Action[9] and in the Tunis phase's Tunis Commitment[10] (paragraphs 15, 24) and Tunis Agenda for the Information Society[11] (paragraphs 39-47, 57-58, 68) — in the latter, notably in the chapter on *Internet Governance*.

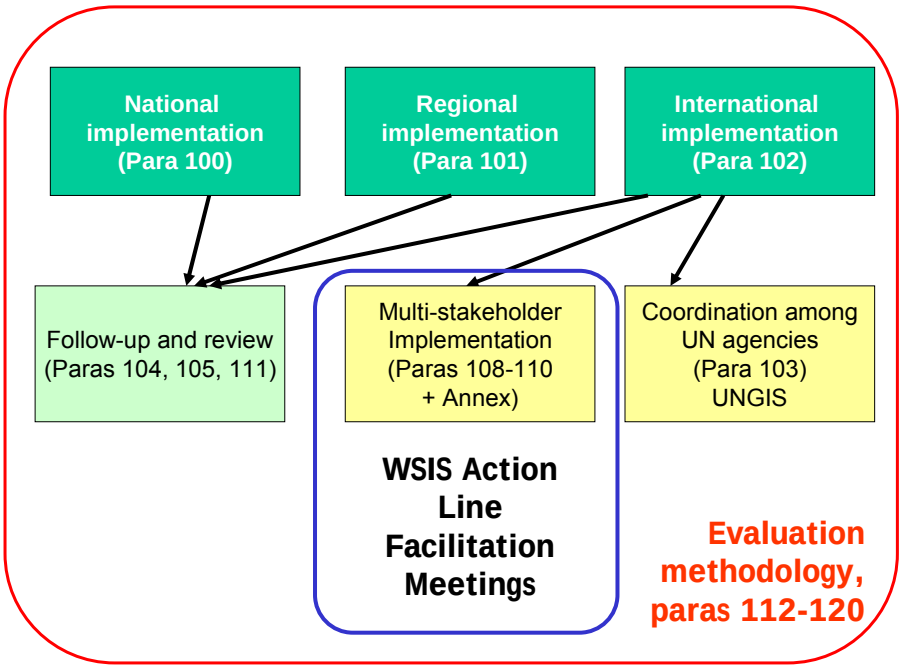
WSIS Implementation and Follow-Up Mechanism

5. The Tunis Agenda also describes the establishment of a mechanism for *implementation* and *follow-up* to WSIS (see Figure 1). A broad framework for the implementation mechanism

at the national, regional and international levels is described in paragraphs 99-102 of the Tunis Agenda. Paragraph 102 deals with implementation at the international level and specifies that it should have both inter-governmental and multi-stakeholder components. Coordination among UN agencies is addressed in paragraph 103, specifically through the UN Group on the Information Society (UNGIS)[12], established in April 2006. Paragraphs 108-110, including the Annex, describe the multi-stakeholder implementation process according to 11 *Action Lines* and the allocation of responsibilities for facilitating WSIS implementation in the different Action Lines. A table showing these Action Lines and the allocation of responsibilities is found in Annex A to this document. ITU is the designated facilitator for Action Line C5: Building confidence and security in the use of ICTs.

6. In order to initiate the overall process, a consultation meeting of potential action line facilitators[13] was held on 24 February 2006, in Geneva. Later, in conjunction with World Telecommunication Day[14] and the inaugural World Information Society Day[15], both on 17 May 2006, a series of Action Line facilitation meetings[16] were held in Geneva. Additional information on the implementation process by Action Line[17] is available on the WSIS website[18].

Figure 1: The framework for WSIS implementation and follow-up



WSIS Action Line C5 Facilitation Meeting on 15-16 May 2006

7. As designated in the Tunis Agenda, ITU is the focal point[19] for facilitating Action Line C5. At the invitation of Yoshio Utsumi[20], ITU Secretary-General, the first consultation on Action Line C5 was organized at ITU Headquarters in Geneva, Switzerland, from 15-16 May 2006. The meeting was organized in conjunction with World Telecommunication Day[21] which had the theme *Promoting Global Cybersecurity*[22].

8. A review of the paragraphs relating to C5 contained in the four WSIS outcome documents[23] demonstrates that Action Line C5 encompasses a broad range of *themes* and *stakeholders*. As emphasized in paragraph 110 of the Tunis Agenda, the "coordination of multi-stakeholder implementation activities would help to avoid duplication of activities. This should include, *inter alia*, information exchange, creation of knowledge, sharing of best practices, and assistance in developing multi-stakeholder and public/private partnerships."

9. The necessity of building partnerships across themes and stakeholders is clearly evident for Action Line C5. In today's interconnected world of global networks, threats can originate anywhere—meaning that national, regional, international cooperation is paramount to

promoting, developing and implementing a global culture of cybersecurity. It was in that spirit that the first C5 meeting had as a theme *Partnerships for Global Cybersecurity.* This meeting focused on exploring potential partnerships among governments, the private sector and other stakeholders, based around the five main themes identified at the 2005 WSIS Thematic Meeting on Cybersecurity[24], comprising: *(1) information-sharing of national approaches, good practices and guidelines*; *(2) developing watch, warning and incident response capabilities*; *(3) technical standards and industry solutions*; *(4) harmonizing national legal approaches and international legal coordination*; and *(5) privacy, data and consumer protection*.

10. The May 2006 Partnerships for Global Cybersecurity C5 meeting website[25] provides links to the final agenda[26], all presentations and contributions[27], the Chairman's Report[28] and audio archives[29]. At this event, the ITU also unveiled a related online reference resource of cybersecurity initiatives and websites worldwide: the ITU Cybersecurity Gateway[30] (see related discussion in this report).

11. During the meeting, a number of actors presented their activities and shared their views on promoting global cybersecurity and cooperation. This Chairman's Report summarizes the discussions throughout the two days and presents a high-level overview of the sessions and speakers below.

Session 1: Meeting Opening and Welcome

12. ITU Deputy Secretary General Mr. Roberto Blois[31] opened the meeting with a speech[32] welcoming the participants, as well as those participating in the meeting through cyberspace, as the meeting was being audiocast live over the internet and archived for future reference. In his opening remarks, the Deputy Secretary General emphasized the challenges involved in creating and promoting a global culture of cybersecurity, highlighting that strategies must be forged through foresight and vision followed by specific action, particularly through strengthened cooperation among the many actors involved. Mr. Blois noted that as facilitator for WSIS Action Line C5 implementation, the ITU looked forward to working closely with all stakeholders in building partnerships to promote global cybersecurity. Mr. Blois then introduced the Chairman of the meeting, Mr. Stein Schjolberg[33], Chief Judge at Moss Tingrett District Court, Norway and Editor of Cybercrimelaw.net[34].

13. In his opening remarks, the Chairman explained that cyberspace is one of the new legal frontiers of our time. Individuals, groups and states now depend on cyberspace for an unprecedented number and level of services. Maintaining the confidentiality, integrity, and availability of the networks and the data they carry increases the trust individuals and groups place in information infrastructures so that they can take full advantage of those services. Increasing trust allows more traditional services to be made available through electronic media and encourages stable development and innovation in new services. Mr. Schjolberg further highlighted the need for standards and laws and argued that only through developing compatible standards and laws can innovation continue to grow. He pointed out that how we shape standards and legal norms of conduct on the internet now will affect millions of people in the future. He also cautioned that standards and laws developed now must include great flexibility in order to account for innovation and new technologies. Unfortunately, subversive actors have found and exploited weaknesses for their own selfish interests, eroding the levels of trust in electronic systems. To combat growth in the misuse of ICTs, states and other actors are responding in a number of ways. Mr. Schjolberg said that in follow-up to the WSIS, we are examining practical methods to strengthen international cooperation and over the next two days we would hear different visions as to how this might be accomplished.

Session 2: World Summit on the Information Society (WSIS) - from Geneva to Tunis

14. In opening this session, Charles Geiger, Executive Director of the WSIS Executive Secretariat[35] provided an overview of WSIS, its outcomes, the 11 WSIS Action Lines and how this relates to Action Line C5 in his presentation WSIS – A Call for Implementation[36]. Mr. Geiger indicated that coordination with groups working on other WSIS Action Lines as well as the Internet Governance Forum[37], also established by the WSIS process, may be needed to move forward pragmatically on implementation.

15. In the next presentation[38], Tim Kelly[39], Head, ITU Strategy and Policy Unit[40], provided an overview of the Consultation Meeting of WSIS action line facilitators that took place on 24 February 2006. One of the main outcomes of the meeting was provisional agreement on the designation of focal points for each of the action lines. In addition to the 48 facilitation roles already defined at WSIS in Tunis, an extra 15 have been defined, including for civil society organizations. Mr. Kelly also made a presentation entitled WSIS Stocktaking Exercise: Building confidence and security in the use of ICTs: The Next Steps[41] which described one of the tools available to assist the WSIS implementation process, the stocktaking database[42], which now has over 3'000 entries. Of these entries, he noted that 695 projects are registered as relating specifically to action line C5.

Session 3: Beyond WSIS - Action Line C5 and Actors

16. This session reviewed the context of Action Line C5: Building confidence and security in the use of ICTs and considered how cybersecurity and critical information infrastructure protection (CIIP) have entered into the national and international security policy agenda and how a number of countries have taken steps to address cybersecurity and CIIP.

17. Robert Shaw[43], Deputy Head, ITU Strategy and Policy Unit[44], gave a presentation on WSIS Outcomes: Building Confidence and Security in the use of ICTs[45]. He set the context for the session by explaining how, in the 21st century, there is a growing dependency on information and communications systems that span the globe. He explained that the rapid growth of ICTs and societal inter-dependency has led to a shift in the perception of threats to cybersecurity since the mid-1990s. Since then, greater linkages have been made between cybersecurity and critical information infrastructure protection (CIIP) and a number of countries have undertaken assessment of the threats, vulnerabilities and mechanisms to redress them. With the growing importance of cybersecurity at the national level, cybersecurity also moved onto the international political agenda. During the WSIS, *Building confidence and security in the use of ICTs* emerged as one of the "key principles" for building an inclusive Information Society.

18. Mr. Shaw explained some of the activities currently being undertaken in the emerging international cooperation agenda. These include the development of the Council of Europe's Convention on Cybercrime[46] (1997-2001); the adoption of UN Resolutions 57/239[47] (2002) and 58/199[48] (2004) on the *Creation of a global culture of cybersecurity and the protection of critical information infrastructure*; ITU Plenipotentiary Resolution 130[49] (2002): *Strengthening the role of ITU in information and communication network security*; WSIS Phase I (2003) Chapter 5 in the Declaration of Principles[50] and Plan of Action[51]: Building confidence and security in the use of ICTs; WSIS Thematic Meeting on Countering Spam (2004)[52]; ITU-T WTSA Resolution 50 (2004): *Cybersecurity*[53]; WSIS Thematic Meeting on Cybersecurity (2005)[54]; WSIS Phase II (2005): Tunis Commitment[55] (paragraphs 15, 24) and Tunis Agenda for the Information Society[56]: Part C on Internet Governance (paragraphs 39-47, 57-58, 68) and the recent adoption of ITU WTDC Resolution 45: *Mechanisms for enhancing cooperation on cybersecurity, including combating spam*[57] (Doha, 2006).

19. Mr. Shaw outlined his view of the key challenges ahead which include: identifying and understanding key cybersecurity themes and identifying relevant actors (e.g. through the ITU Cybersecurity Gateway[58]); engaging 'siloed' communities in dialogue who may not otherwise talk with each other; and creating a platform for enhanced multi-stakeholder collaboration and partnerships. He explained the background of the *themed* approach adopted for the meeting (derived from the WSIS Thematic Meeting on Cybersecurity (2005)[59]).

20. In the following talk, Isabelle Abele-Wigert[60], Research Fellow at the Center of Security Studies, Swiss Federal Institute of Technology[61], gave a presentation on Challenges Governments Face in the Field of CIIP - Stakeholders and Perspectives outlining the main findings of their 2006 Critical Information Infrastructure Protection (CIIP) Handbook[62]. From her comparative analysis of the main actors and different perspectives in the field of CIIP, Ms. Abele-Wigert identified the main challenges governments face in the protection of critical information infrastructures and cybersecurity. She explained that, as there is no wide agreement on what CIIP should include, what needs to be protected and by whom, there are often conflicting viewpoints, which in turn hamper the development and implementation of an effective national CIIP policy. She stated that governments need to consider the perspectives

of key actors to formulate effective CIIP policy and collaboration. In some countries, focal point CIIP organizations have been established and tasked with specific coordination tasks.

21. In her summary, she put forward the main roles governments could adopt in promoting cybersecurity. These include: activities for assessing risks and threats; enhancing vulnerability detection and response; promoting more secure products and services; raising overall awareness and information-sharing; developing an adequate legal framework; and emergency preparedness and crisis management. She also emphasized that effective national protection policies have to be supported with efforts in the international arena. She noted that as CIIP has global implications, transnational institutions are necessary to make progress in addressing the key challenges.

Session 4: Perspectives on Promoting Global Cybersecurity

22. A globally interconnected network means that cybersecurity cannot be effectively addressed by individual nations; it requires a combined effort by all countries worldwide. Session 4 focused on sharing perspectives as to how cybersecurity and critical information infrastructure protection (CIIP) can be best approached at the national, regional and international levels. In his opening remarks, Seymour Goodman[63], Professor at the Georgia Institute of Technology[64] and chair of Session 4, observed how, in cyberspace, all countries are adjacent to each other and most countries are relatively less developed and rather defenseless. Mr. Goodman continued by questioning if we were really making progress on the issues and noted that a major challenge is raising consciousness and persuading national and regional leadership to commit to and buy-in to fighting this conflict. This is an important problem for which proper defense requires a sustained global effort.

23. No single nation can successfully secure itself in isolation, said Michele Markoff[65], Senior Coordinator for International Critical Infrastructure Protection with the Bureau of Political Military Affairs, U.S. State Department[66]. Each nation's security is limited by that of the weakest link in this global infrastructure, she continued. She said it is critical to build awareness at a national policy level of the importance of cyber or critical information infrastructure protection. There is a need for national action and international cooperation to build a global culture of cybersecurity. She identified the issues that need to be addressed as: the need to survey and catalogue what each party sees as the key issues faced by national policy-makers; a survey of the sources of information and assistance related to building a global culture of cybersecurity; the sources of best practices; the unique challenges faced by developing countries in addressing security of networks; and how to establish watch warning and incident response recovery capability.

24. Key challenges for cybersecurity include improved dialogue between national departments, national departments of justices and Interpol—however, identifying relevant actors and getting them to talk together has proven to be challenging. Ms. Markoff proposed a U.S. framework for national action[67] with a model national plan Part 1[68] and Part 2[69] to respond to the challenges associated with building a culture of cybersecurity. She said that government should lead with a national plan and national strategy for cybersecurity to protect critical infrastructures. She said that if government leads, the private sector, individuals and SMEs will follow. Once the national government has a plan and strategy in place, they should reach out regionally and internationally to find out how they can best interact with their counterparts elsewhere.

25. Ms. Markoff stated that the key activity of any nation is to ensure that there are adequate, substantive and procedural laws that take into account the need to be able to adequately prosecute the misuse of information technologies. She noted that work on cybersecurity has already begun in a large number of areas: the Council of Europe's Convention on Cybercrime[70]; United Nations' resolutions (e.g., 57/239[71] (2002) and 58/199[72] (2004)); Resolutions from ITU Plenipotentiary Conferences[73]; at the World Telecom Standardization Assembly (WTSA)[74], WSIS meetings; and other initiatives. Markoff pointed out that what remains to be done—and she emphasized there is much to be done—is to devise the best way to organize, either nationally, regionally, internationally, to have the best impact on prevention of damage to our critical information infrastructures. She also noted: "More and more, we recognize that it is the individual user that we have to inculcate with this culture of security, all the way up through enterprises, industries and national governments."

26. In the following talk, Andrea Pirotti, Executive Director[75] of the European Network and Information Security Agency (ENISA)[76], presented ENISA's contribution to the development of Network and Information Security within the Community[77] and provided an overview of ENISA's mandate and ongoing and planned security activities in European countries. He emphasized that European Union Member States set up ENISA to help develop a culture of network and information security for the benefit of the citizens, consumers, enterprises and public sector organizations.

27. The European Schoolnet[78] and Safer Internet Programme[79] are part of the European approach to cybersecurity, which is an integral part of information security. Janice Richardson[80], Insafe Project Manager, emphasized the need for a coordinated approach in her presentation Insafe: a European approach to cyber-safety[81], taking advantage of possible synergies and avoiding duplication of work through providing a common platform for cybersecurity.

Session 5: National Legal Approaches and International Legal Coordination for Global Cybersecurity

28. Appropriate legislation and enforcement are two key elements in building trust in cyberspace. The development of cyberspace has created a new environment for criminal offences as online offences. But it may also create problems in the application of the penal legislation. Many countries have amended their penal codes or are in the process of adopting amendments, in accordance with standards and obligations in international conventions and recommendations. This session reviewed the national legal approaches adopted currently and areas for potential coordination in international laws.

29. In the first talk, Chairman Schjolberg[82], in his presentation on Building Trust — National Legal Approaches and International Legal Coordination for Global Cybersecurity[83], shared an overview on the main actors and instruments making up the global legal framework for cybercrime.

30. On the legal and legislative drafting and capacity fronts, there is actually a fairly small world out there, said Betty-Ellen Shave[84], Assistant Deputy Chief for International Computer Crime in the Computer Crime and Intellectual Property Section (CCIPS) of the U.S. Department of Justice[85]. Ms. Shave presented U.S. international efforts related to training and other ongoing international collaboration. She highlighted that there are numerous efforts also undertaken by other countries and organizations to offer training on challenges related to cybercrime. She noted that the U.S. currently offers training on how to draft a usable cybercrime statute, based on the Council of Europe's Convention on Cybercrime[86], as well as offering investigative capacity-building consisting mainly of practical and technically-oriented training for police officers. The role of conscious-raising training for policy-makers was also emphasized. Additional courses are currently being planned and scheduled in all regions of the world. Ms. Shave also mentioned further cooperation planned with the Council of Europe.

31. Guidelines alone are not sufficient to fight cybercrime, stated Margaret Killerby[87], Head of the Department of Crime Problems at the Council of Europe[88] in her presentation, The Convention on Cybercrime[89]. Bilateral agreements are too numerous and complicated, she said: "we need an international instrument which is practical and widely accepted and of course, we already have one." She noted that a number of countries are currently considering becoming party to the Council of Europe's Convention on Cybercrime[90]. "We are looking at a Convention which we fully and confidently expect to receive widespread, worldwide support", Mrs. Killerby continued.

32. Mark Goodman[91], Senior Advisor for the Interpol Steering Committee on Information Technology Crime[92], shared information on Interpol's role in fighting high tech crime in his presentation entitled Interpol's Role in Fighting High-Tech Crime[93]. He said that technological developments have shrunk the world down to a global village and there are now no national boundaries. With the escalation of serious transnational crime, the need for a global police co-operation response has never been more acute. Interpol aims to provide a unique range of essential services for the law enforcement community to optimize international efforts to combat cybercrime and cyberterrorism.

Session 6: Perspectives on Promoting Global Cybersecurity (Session 4 cont'd)

33. The second day of the meeting opened with Session 6 presenting additional perspectives on the theme of World Telecommunication Day 2006: *Promoting Global Cybersecurity*. Art Reilly[94] from Cisco Systems, speaking on behalf of the International Chamber of Commerce (ICC)[95], gave a presentation entitled A Business Perspective on Promoting Cybersecurity[96]. Mr. Reilly summarized his talk by noting that all stakeholders have a role to play in creating a culture of cybersecurity; business has a broad role, due to its wide range of activities in the Information Society; cooperation among all stakeholders is important; ICC stands ready to organize, participate and facilitate in such cooperative activities; and security is a continuing process, not a one-time solution. He also said that raising security awareness is in the business sector's interest as this promotes global connectivity and security is an essential building block in the development of trust and confidence in ICTs.

34. Sarah Andrews[97], Policy Analyst for Consumer Policy, Privacy and Information Security at the Organisation for Economic Co-operation and Development (OECD) gave a presentation entitled The OECD Trust Agenda: Promoting Security and Confidence[98] that outlined the OECD's multiple activities in promoting security and confidence in the use of ICTs. These activities include: the OECD's Guidelines for the Security of Information Systems and Networks[99] (2002); Guidelines on the Protection of Privacy and Transborder Flows of Personal Data[100] (1980/1998); Privacy Online: OECD Guidance on Policy and Practice[101] (2002); Consumer Protection Guidelines[102] (1999); Guidelines for Protecting Consumers from Cross-Border Fraud[103] (2003); The OECD Anti-Spam Toolkit; and a recent Scoping Study on the Measurement of Trust in the Online Environment (2005).

35. In the next talk, Bertrand de la Chapelle[104], on behalf of the WSIS Privacy and Security Working Group, gave a presentation on Digital Identity and Privacy[105] describing a user-centric approach for the trust framework. He asked how do we guarantee that new systems of digital privacy and identity will center identity on the individual, foster privacy, and enable public participation in their design and application? He identified some of the main technologies, initiatives and actors in this field. Mr. de la Chapelle said we should aim for a global privacy protection framework that takes the form of a legally binding instrument. He also emphasized the need for a balanced approach in maintaining security and protecting privacy.

Session 7: Partnerships for Developing Watch, Warning and Incident Response Capabilities

36. Suresh Ramasubramanian[106], Postmaster at Outblaze Limited[107] and Coordinator for APCAUCE.ORG[108], chaired the session on establishing partnerships for developing watch, warning and incident response capabilities. In his presentation entitled Shared Incident Response Shared Incident Response—towards mitigation of spam and net abuse[109], he shared his views on current developments in spam sources, botnet abuse and future trends in incident response. He emphasized the need for active cooperation with law enforcement in different countries and noted that this requires quick reaction. He sees the need for standardization of online contact mechanisms, secure online transmission of subpoenas and digitally signed emails instead of faxes or certified mail. He further stated that while personal relations with individual law enforcement agents can be useful, there is no substitute for official points of contact.

37. Ahmed Sindi, Deputy Governor, Communication and Information Technology Commission (CITC)[110], Saudi Arabia, made a presentation entitled Cyber Security Initiatives in Saudi Arabia[111] reviewing Saudi Arabia's internet and telecom demographics and its response to cyber-threats, including plans to establish a national CERT. In response to its mandate, CITC has researched and investigated other international CERT initiatives, held information gathering sessions with relevant individuals and organizations and sought input from reputable organizations.

38. John Harrison[112], Consultant to the United Kingdom's National Infrastructure Security Co-ordination Centre (NISCC)[113] introduced the concept of WARPs (Warning, Advice and Reporting Points)[114] in his presentation[115]. WARPs are part of the NISCC's information-sharing strategy to protect the United Kingdom's Critical National Infrastructure from electronic

attacks. He stated that WARPs have been shown to be effective in improving information security by stimulating better communication of alerts and warnings, improving awareness and education, and encouraging incident reporting. The WARP Toolbox can be downloaded freely from a dedicated website at http://www.warp.gov.uk.

39. Tomas Lamanauskas[116], Deputy Director of the Communications Regulatory Authority (RRT) of the Republic of Lithuania[117] shared his insights on recent activities and initiatives undertaken in Lithuania in his presentation, Direction to Success: Public and Private Sectors Partnership[118]. A government resolution from March 2005 called for the creation of a CERT within RRT before the end of 2006. The rationale behind the creation of this main CERT is to provide the numerous CERT teams in the country with a coordination centre and a general contact point in the country. Mr. Lamanauskas emphasized in his presentation that efforts would be devoted to consolidation and cooperation and the integration of different incident reporting and response efforts in Lithuania.

40. Nabil Sahli[119], Head of the CERT/TCC, the Tunisian National Agency for Computer Security[120], representing the Tunisian Ministry of Communication Technologies[121], shared his insights into the Tunisian experience and strategy in the establishment of national watch, warning and incident response capabilities in his presentation Insights into the Tunisian experience and strategy in the establishment of national watch, warning and incident response capabilities[122]. Mr. Sahli further explored collaborative approaches to assist developing economies for the establishment of national and regional CSIRTs (Computer Security Incident Response Teams).

Session 8: ITU Contributions to Promoting Partnerships for Global Cybersecurity

41. Session 8 provided an overview of several specific ITU contributions to promoting global cybersecurity.

42. Alexander Ntoko[123], Chief of the ITU-D E-Strategies Unit, opened the session with a report on discussions at the recent 2006 ITU World Telecommunication Development Conference (WTDC). The gap is enormous between cybersecurity in developing and developed nations, Mr. Ntoko noted, mentioning that ITU is slowly working towards putting in place a framework for collaboration amongst its Member States. Discussions on cybersecurity and spam brought up during the negotiations in WTDC Resolution 45: *Mechanisms for enhancing cooperation on cybersecurity, including combating spam*[124] (Doha, 2006), focused on the need for cooperation and collaboration and developing a common understanding on issues of spam and cyber-threats.

43. On the occasion of World Telecommunication Day 2006[125] and the first World Information Society Day 2006[126] dedicated to the theme of *Promoting Global Cybersecurity*, Christine Sund[127], Policy Analyst, ITU Strategy and Policy Unit[128], unveiled the ITU Cybersecurity Gateway[129]. She noted that both national actors and the international community recognize the importance of using online technologies for information sharing among developed and developing countries.

44. Finding information on relevant actors and the right partners in a highly complex field such as cybersecurity is, however, not always that easy, stated Ms. Sund. The ITU Cybersecurity Gateway[130] is a global online reference resource of national cybersecurity initiatives and websites around the world, as well as sharing other cybersecurity-related information and resources. The portal presents information tailored to four specific audiences: citizens, businesses, governments, and international organizations. The portal also provides information resources on current topical cybersecurity concerns such as spam, spyware, phishing, scams and frauds, worms and viruses, denial of service attacks, etc.

45. Ms. Sund stated that with the Cybersecurity Gateway, ITU aims to open the door to a more focused discussion on the roles and responsibilities of the cybersecurity actors and what immediate collaborative actions could be taken to build and promote a global culture of cybersecurity. With thousands of links to relevant materials and actors, ITU will constantly update the portal with information on cybersecurity initiatives and resources gathered from contributors around the globe. As one example, a number of countries have begun national critical information infrastructure protection (CIIP) programmes and sharing these different

approaches through the portal can assist both developed and developing economies in developing their own CIIP strategies.

46. Georges Sebek, Counsellor for ITU-T Study Group 17 (SG17)[131], gave a presentation entitled ITU-T Work on Security[132] which reviewed the more recent activities of SG 17. SG 17 is the lead ITU study group on telecommunication security and is responsible for coordination of security across all different ITU-T study groups. Among other things, Mr. Sebek described the establishment of a Focus Group on Security Baseline for Network Operators[133] in October 2005. The immediate next steps for the Focus Group include surveying network operators by means of a questionnaire. Mr. Sebek also explained current work in progress in SG17 on an ICT security standards roadmap. This roadmap includes four parts: Part 1 contains information about organizations working on ICT security standards; Part 2 is a database of existing security standards; Part 3 will be a list of standards in development; and Part 4 will identify future needs and proposed new standards

47. Benoît Morel[134], Professor at Carnegie Mellon University[135], provided a presentation entitled A Methodology for Measuring the Capability to Counter Cybersecurity-related Offenses[136].

Session 9: Partnerships for Global Cybersecurity – The Way Forward

48. This session, chaired by the event Chairman Judge Schjolberg[137], reviewed some of the different initiatives and perspectives presented during the C5 facilitation meeting and asked participants to discuss their proposals for specific future cooperative measures. Chairman Schjolberg noted in particular that he saw a pressing and important need for capacity-building on the harmonization of cybercrime legislation and in particular on specifically contributing to the ratifications, accessions, and implementation of the principles and standards of the Council of Europe's Convention on Cybercrime[138].

49. Robert Shaw[139], Deputy Head, ITU Strategy and Policy Unit[140] and focal point[141] at ITU for C5 follow-up gave a brief presentation[142] setting out ideas for the way forward. He noted that the paragraphs relating to C5 contained in the four WSIS outcome documents[143] show that Action Line C5: *Building confidence and security in the use of ICTs* encompasses a broad range of *themes* and *actors* and that a first step was to identify and understand these. This could be done through surveys and research and the ITU Cybersecurity Gateway[144] provided one possible mechanism toward that goal. He noted other challenges were to engage 'siloed' communities who may not normally talk with each other and creating a platform for enhanced multi-stakeholder collaboration and partnerships with limited bureaucracy and reduced "transaction costs".

50. He reviewed the proposed themed approach for approaching cybersecurity and CIIP derived from the 2005 WSIS Thematic Meeting on Cybersecurity and also used in the ITU Cybersecurity Gateway[145], but noted that other approaches were also possible and have been discussed during the meeting. In relation to this, he noted the presentation Challenges Governments Face in the Field of CIIP - Stakeholders and Perspectives by Isabelle Abele-Wigert[146] which referred to the main findings of their 2006 Critical Information Infrastructure Protection (CIIP) Handbook[147] discussing different *perspectives* of *system-level, technical*; *business*; *law-enforcement*; and *national-security perspectives*. He also referred to Michele Markoff's[148] presentation, which outlined a proposed U.S. framework for national action[149] and the associated model national plan (Part 1[150] and Part 2[151]). This used an approach for a *model national plan* through a *national strategy*; *legal foundation and regulatory development*; *incident response, watch, warning, recovery*; *partnerships between industry and government*; and promotion of a *culture of security*.

51. He reviewed paragraph 110 of the Tunis Agenda[152] which stated that "coordination of multi-stakeholder implementation activities would help to avoid duplication of activities. This should include, *inter alia*, information exchange, creation of knowledge, sharing of best practices, and assistance in developing multi-stakeholder and public/private partnerships."

52. Based on the discussions by experts presented during the two day event, a few pragmatic next steps could be envisioned, including enhancement of the ITU Cybersecurity Gateway[153] to assist in a survey of themes and actors; the creation of sub-groups on specific themes; the planning of the next meeting (including whether it should be global or regional);

the use of electronic tools for further discussion; and what should be the relationship and coordination of C5 activity vis-à-vis the Internet Governance Forum[154] and ITU cybersecurity activities (e.g., in WTDC Resolution 45: *Mechanisms for enhancing cooperation on cybersecurity, including combating spam*[155] (Doha, 2006) and ITU-T Work on Security[156]).

53. Following general discussion and a review of the presentations made by experts during the event, Mr. Shaw suggested that an initial set of *three focus areas* have emerged, as described below.

54. He said the first proposed focus area relates to *information-sharing of national approaches, good practices and guidelines* and more specifically, what approaches national policy-makers might take to address cybersecurity and CIIP at the national level. For example, examining the common elements in various national approaches could lead to a *first focus area* on the *development of a generic model framework or toolkit that national policy-makers could use to develop and implement a national cybersecurity or CIIP programme*.

55. He said the second proposed focus area relates to *harmonizing national legal approaches and international legal coordination*. For example, in Chairman Schjolberg's opening remarks, he referred to an important need for capacity-building on the harmonization of cybercrime legislation and, in particular, on specifically contributing to the ratifications, accessions, and implementation of the principles and standards of the Council of Europe's Convention on Cybercrime[157]. Therefore, a *second focus area* could be *capacity-building on the harmonization of cybercrime legislation, the Council of Europe's Convention on Cybercrime*[158], *and enforcement*.

56. The third proposed focus area relates to *developing watch, warning and incident response capabilities*. In particular, as discussed in the five presentations in Session 7, there is a clear requirement for sharing knowledge and expertise on national watch, warning and incident response capabilities. It was also noted that Nabil Sahli[159], Head of the CERT/TCC, the Tunisian National Agency for Computer Security[160], in his presentation entitled Insights into the Tunisian experience and strategy in the establishment of National watch, warning and Incident Response capabilities[161] stated that they are ready to host a multi-stakeholder meeting to assist developing countries on this topic in Tunisia, in collaboration with ITU and other international organizations. Therefore, a *third focus area* could be information-sharing of best practices on *developing watch, warning and incident response capabilities*.

Session 10: Close of Meeting

57. At the close of the meeting, a statement[162] was made by the representative of the Russian Federation, who stated "it is important to examine the issue of international information security, which encompasses, inter alia, such interrelated topics as spam, cybercrime, cybersecurity, hostile use of ICTs by states or governments that undermine stability and security of the Internet". Reviewing these topics, the Russian Federation further proposed "to examine the topic of international information security in a comprehensive manner, including the issues of cybersecurity, spam, the threats of cybercrime, cyberterrorism, and hostile use of the Internet infrastructure and potential by states or governments."

58. Chairman Judge Schjolberg[163], in closing the meeting, thanked the participants and staff of the ITU for their support in organizing the meeting. Mr. Shaw thanked Mr. Scholberg for his able chairmanship and said that the Chairman's report would be circulated for review and comments by the participants. He also indicated that, as C5 facilitator, ITU would put forward a more detailed project proposal for follow-up on the three initial focus areas discussed in Session 9 above for endorsement by the participants.

Additional Meeting Notes

59. Acknowledgement is also made of the following written contributions to the meeting:

- Contribution from the Ministry of Communication and Information Technology, Indonesia, May 2006: National Cybersecurity Policy & Implementation for Government of Indonesia[164]

- Statement by the Representative of the Russian Federation at the C5 Facilitation Meeting, 16 May 2006: Contribution from the Russian Federation[165]
- Study on "A Methodology for Measuring the Capability to Counter Cybersecurity-related Offenses": by Benoît Morel, Carnegie Mellon University: A Methodology for Measuring the Capability to Counter Cybersecurity-related Offenses[166]

ANNEX A

C1. The role of stakeholders	UN DESA
C2. Information and communication infrastructure	ITU
C3. Access to information and knowledge	UNESCO
C4. Capacity building	UNDP
C5. Building confidence and security in the use of ICTs	ITU
C6. Enabling environment	UNDP
C7. ICT applications ▪E-government ▪E-business ▪E-learning ▪E-health ▪E-employment ▪E-environment ▪E-agriculture ▪E-science	 UN DESA UNCTAD UNESCO WHO ILO WMO FAO UNESCO
C8. Cultural diversity and identity, linguistic diversity and local content	UNESCO
C9. Media	UNESCO
C10. Ethical dimensions of the Information Society	UNESCO
C11. International and regional cooperation	UN DESA

[1] http://www.itu.int/wsis/

[2] http://www.itu.int/officials/Utsumi.html

[3] http://www.itu.int/newsroom/wtd/2006/

[4] http://www.itu.int/newsroom/wtd/2006/index.html

[5] http://www.itu.int/wsis/

[6] http://www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=2316|0

[7] http://www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=1161|0

[8] Ibid

[9] http://www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=1160|0

[10] http://www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=2266|0

[11] http://www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=2267|0

[12] http://www.unqis.org

[13] http://www.itu.int/wsis/implementation/consultation24feb.html

[14] http://www.itu.int/newsroom/wtd/2006/

[15] http://www.itu.int/wisd/

[16] http://www.itu.int/wsis/implementation/meetings.html

[17] http://www.itu.int/wsis/implementation/index.html

[18] http://www.itu.int/wsis/

[19] http://www.itu.int/wsis/c5/

[20] http://www.itu.int/officials/Utsumi.html

[21] http://www.itu.int/newsroom/wtd/2006/

[22] http://www.itu.int/newsroom/wtd/2006/index.html

[23] http://www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=2316|0

[24] http://www.itu.int/osg/spu/cybersecurity/2005/index.phtml

[25] http://www.itu.int/osg/spu/cybersecurity/2006/

[26] http://www.itu.int/osg/spu/cybersecurity/2006/agenda.html

[27] http://www.itu.int/osg/spu/cybersecurity/2006/presentations.html

[28] http://www.itu.int/osg/spu/cybersecurity/2006/chairmansreport.pdf

[29] http://www.itu.int/ibs/sg/spu/200605cybersecurity/index.html

[30] http://www.itu.int/cybersecurity/

[31] http://www.itu.int/officials/Blois.html

[32] http://www.itu.int/osg/spu/cybersecurity/2006/presentations/c5-opening-remarks-blois.pdf

[33] http://www.itu.int/osg/spu/cybersecurity/2006/speaker_bios.html#schjolberg0

[34] http://www.cybercrimelaw.net

[35] http://www.itu.int/osg/spu/cybersecurity/2006/speaker_bios.html#geiger

[36] http://www.itu.int/osg/spu/cybersecurity/2006/presentations/geiger-wsis-15-may-2006.pdf

[37] http://www.intgovforum.org

[38] http://www.itu.int/osg/spu/cybersecurity/2006/presentations/report-on-facilitators-meeting-kelly.pdf

[39] http://www.itu.int/osg/spu/cybersecurity/2006/speaker_bios.html#kelly

[40] http://www.itu.int/osg/spu/

[41] http://www.itu.int/osg/spu/cybersecurity/2006/presentations/kelly-wsis-stocktaking-15-may-2006.pdf

[42] http://www.itu.int/wsis/stocktaking/scripts/search.asp

[43] http://www.itu.int/osg/spu/cybersecurity/2006/speaker_bios.html#shaw

[44] http://www.itu.int/osg/spu/

[45] http://www.itu.int/osg/spu/cybersecurity/2006/presentations/shaw-c5-consultation-15-may-2006.pdf

[46] http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm

[47] http://www.itu.int/osg/spu/cybersecurity/docs/UN_resolution_57_239.pdf

[48] http://www.itu.int/osg/spu/cybersecurity/docs/UN_resolution_58_199.pdf

[49] http://www.itu.int/aboutitu/basic-texts/resolutions/res130.html

[50] http://www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=1161|0

[51] http://www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=1160|0

[52] http://www.itu.int/osg/spu/spam/meeting7-9-04/index.html

[53] http://www.itu.int/ITU-T/wtsa/resolutions04/Res50E.pdf

[54] http://www.itu.int/osg/spu/cybersecurity/2006/index.phtml

[55] http://www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=2266|0

[56] http://www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=2267|0

[57] http://www.itu.int/ITU-D/wtdc06/pdf/wtdc06-finalreport.pdf

[58] http://www.itu.int/cybersecurity/

[59] http://www.itu.int/osg/spu/cybersecurity/2006/index.phtml

[60] http://www.itu.int/osg/spu/cybersecurity/2006/speaker_bios.html#wigert

[61] http://www.css.ethz.ch/index_EN

[62] http://www.crn.ethz.ch/research/CIIP.cfm

[63] http://www.itu.int/osg/spu/cybersecurity/2006/speaker_bios.html#goodmans

[64] http://www.spp.gatech.edu/faculty/faculty/sgoodman.php

[65] http://www.itu.int/osg/spu/cybersecurity/2006/speaker_bios.html#markoff

[66] http://www.state.gov/t/pm/ppa/icipt/

[67] http://www.itu.int/osg/spu/cybersecurity/2006/presentations/markoff-framework-for-national-action-15-may-2006.pdf

[68] http://www.itu.int/osg/spu/cybersecurity/2006/presentations/markoff-part1-15-may-2006.pdf

[69] http://www.itu.int/osg/spu/cybersecurity/2006/presentations/markoff-part2-15-may-2006.pdf

[70] http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm

[71] http://www.itu.int/osg/spu/cybersecurity/docs/UN_resolution_57_239.pdf

[72] http://www.itu.int/osg/spu/cybersecurity/docs/UN_resolution_58_199.pdf

[73] http://www.itu.int/plenipotentiary/

[74] http://www.itu.int/ITU-T/wtsa-04/

[75] http://www.itu.int/osg/spu/cybersecurity/2006/speaker_bios.html#pirotti0

[76] http://www.enisa.eu.int/

[77] http://www.itu.int/osg/spu/cybersecurity/2006/presentations/pirotti-enisa-15-may-2006.pdf

[78] http://www.eun.org/

[79] http://www.saferinternet.org/

[80] http://www.itu.int/osg/spu/cybersecurity/2006/speaker_bios.html#richardson

[81] http://www.itu.int/osg/spu/cybersecurity/2006/presentations/richardson-15-may-2006.pdf

[82] http://www.itu.int/osg/spu/cybersecurity/2006/speaker_bios.html#schjolberg0

[83] http://www.itu.int/osg/spu/cybersecurity/2006/presentations/schjolberg-15-may-2006.pdf

[84] http://www.itu.int/osg/spu/cybersecurity/2006/speaker_bios.html#shave

[85] http://www.cybercrime.gov/

[86] http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm

[87] http://www.itu.int/osg/spu/cybersecurity/2006/speaker_bios.html#killerby

[88] http://www.coe.int/T/E/Legal_affairs/Legal_co-operation/Combating_economic_crime/

[89] http://www.itu.int/osg/spu/cybersecurity/2006/presentations/killerby-15-may-2006.pdf

[90] http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm

[91] http://www.itu.int/osg/spu/cybersecurity/2006/speaker_bios.html#goodmanm

[92] http://www.interpol.int/Public/TechnologyCrime/default.asp

[93] http://www.itu.int/osg/spu/cybersecurity/2006/presentations/goodman-interpol-15-may-2006.pdf

[94] http://www.itu.int/osg/spu/cybersecurity/2006/speaker_bios.html#reilly

[95] http://www.iccwbo.org/

[96] http://www.itu.int/osg/spu/cybersecurity/2006/presentations/reilly-icc-cisco-16-may-2006.pdf

[97] http://www.itu.int/osg/spu/cybersecurity/2006/speaker_bios.html#andrews

[98] http://www.itu.int/osg/spu/cybersecurity/2006/presentations/andrews-oecd-16-may-2006.pdf

[99] http://www.oecd.org/document/42/0,2340,en_2649_34255_15582250_1_1_1_1,00.html

[100] http://www.oecd.org/document/57/0,2340,en_2649_34255_1815186_1_1_1_1,00.html

[101] http://www.oecd.org/document/49/0,2340,en_2649_34255_19216241_1_1_1_1,00.html

[102] http://www.oecd.org/document/51/0,2340,en_2649_34267_1824435_1_1_1_1,00.html

[103] http://www.oecd.org/document/50/0,2340,en_2649_34267_2514994_1_1_1_1,00.html

[104] http://www.itu.int/osg/spu/cybersecurity/2006/speaker_bios.html#delachapelle

[105] http://www.itu.int/osg/spu/cybersecurity/2006/presentations/de-la-chapelle-digital-identity-16-may-2006.pdf

[106] http://www.itu.int/osg/spu/cybersecurity/2006/speaker_bios.html#ramasubramanian

[107] http://www.outblaze.com

[108] http://www.apcauce.org

[109] http://www.itu.int/osg/spu/cybersecurity/2006/presentations/ramasubramanian-16-may-2006.pdf

[110] http://www.citc.gov.sa/

[111] http://www.itu.int/osg/spu/cybersecurity/2006/presentations/sindi-saudi-arabia.pdf

[112] http://www.itu.int/osg/spu/cybersecurity/2006/speaker_bios.html#harrison

[113] http://www.niscc.gov.uk/niscc/index-en.html

[114] http://www.warp.gov.uk/

[115] http://www.itu.int/osg/spu/cybersecurity/2006/presentations/harrison-warps-16-may-2006.pdf

[116] http://www.itu.int/osg/spu/cybersecurity/2006/speaker_bios.html#lamanauskas

[117] http://www.rrt.lt/

[118] http://www.itu.int/osg/spu/cybersecurity/2006/presentations/lamanauskas-16-may-2006.pdf

[119] http://www.itu.int/osg/spu/cybersecurity/2006/speaker_bios.html#sahli

[120] http://www.ansi.tn/

[121] http://www.infocom.tn/

[122] http://www.itu.int/osg/spu/cybersecurity/2006/presentations/sahli-tunisia-16-may-2006.pdf

[123] http://www.itu.int/osg/spu/cybersecurity/2006/speaker_bios.html#ntoko

[124] http://www.itu.int/ITU-D/wtdc06/pdf/wtdc06-finalreport.pdf

[125] http://www.itu.int/newsroom/wtd/2006/

[126] http://www.itu.int/wisd/2006/

[127] http://www.itu.int/osg/spu/cybersecurity/2006/speaker_bios.html#sund

[128] http://www.itu.int/osg/spu/

[129] http://www.itu.int/cybersecurity/

[130] Ibid

[131] http://www.itu.int/ITU-T/studygroups/com17/

[132] http://www.itu.int/osg/spu/cybersecurity/2006/presentations/sebek-tsb-16-may-2006.pdf

[133] http://www.itu.int/ITU-T/studygroups/com17/sbno/

[134] http://www.itu.int/osg/spu/cybersecurity/2006/speaker_bios.html#morel

[135] http://www.cmu.edu/

[136] http://www.itu.int/osg/spu/cybersecurity/2006/presentations/morel-methodology-for-measuring-16-may-2006.pdf

[137] http://www.itu.int/osg/spu/cybersecurity/2006/speaker_bios.html#schjolberg0

[138] http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm

[139] http://www.itu.int/osg/spu/cybersecurity/2006/speaker_bios.html#shaw

[140] http://www.itu.int/osg/spu/

[141] http://www.itu.int/wsis/c5/index.html

[142] http://www.itu.int/osg/spu/cybersecurity/2006/presentations/shaw-c5-consultation-next-steps-16-may-2006.pdf

[143] http://www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=2316|0

[144] http://www.itu.int/cybersecurity/

[145] Ibid

[146] http://www.itu.int/osg/spu/cybersecurity/2006/speaker_bios.html#wigert

[147] http://www.crn.ethz.ch/research/CIIP.cfm

[148] http://www.itu.int/osg/spu/cybersecurity/2006/speaker_bios.html#markoff

[149] http://www.itu.int/osg/spu/cybersecurity/2006/presentations/markoff-framework-for-national-action-15-may-2006.pdf

[150] http://www.itu.int/osg/spu/cybersecurity/2006/presentations/markoff-part1-15-may-2006.pdf

[151] http://www.itu.int/osg/spu/cybersecurity/2006/presentations/markoff-part2-15-may-2006.pdf

[152] http://www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=2267|0

[153] http://www.itu.int/cybersecurity/

[154] http://www.intgovforum.org

[155] http://www.itu.int/ITU-D/wtdc06/pdf/wtdc06-finalreport.pdf

[156] http://www.itu.int/osg/spu/cybersecurity/2006/presentations/sebek-tsb-16-may-2006.pdf

[157] http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm

[158] http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm

[159] http://www.itu.int/osg/spu/cybersecurity/2006/speaker_bios.html#sahli

[160] http://www.ansi.tn/

[161] http://www.itu.int/osg/spu/cybersecurity/2006/presentations/sahli-tunisia-16-may-2006.pdf

[162] http://www.itu.int/osg/spu/cybersecurity/2006/contribution-russian-federation.pdf

[163] http://www.itu.int/osg/spu/cybersecurity/2006/speaker_bios.html#schjolberg0

[164] http://www.itu.int/osg/spu/cybersecurity/2006/contribution-building-national-cybersecurity-indonesia.pdf

[165] http://www.itu.int/osg/spu/cybersecurity/2006/contribution-russian-federation.pdf

[166] http://www.itu.int/osg/spu/cybersecurity/2006/morel-paper-15-may-2006.pdf