ITU WSIS THEMATIC MEETING ON CYBERSECURITY

ITU Headquarters, Geneva, Switzerland
28 June – 1 July 2005

CHAIRMAN'S REPORT
Version 2.0

1. At the invitation of Yoshio Utsumi[1], ITU Secretary-General, an ITU WSIS Thematic Meeting on Cybersecurity[2] was held at ITU Headquarters in Geneva, Switzerland, from 28 June to 1 July 2005. The event was organized in the framework of the implementation of the Declaration of Principles and Plan of Action[3] adopted on 12 December 2003, at the first phase of the World Summit on the Information Society (WSIS)[4] and in preparation for the Tunis phase of WSIS, to be held from 16 to 18 November, 2005.

2. The event website[5] provides links to the final agenda[6], all background papers[7], presentations[8], electronic contributions[9], the Chairman's Report[10] and audio archives[11]. The website contains a wealth of related materials and in itself provides a valuable resource for the future.

3. The four-day meeting was structured to consider and debate six broad themes in promoting international dialogue and cooperative measures among governments, the private sector and other stakeholders as well as promotion of a global culture of cybersecurity. These include information sharing of national and regional approaches, good practices and guidelines[12]; developing watch, warning and incident response capabilities[13]; technical standards and industry solutions[14]; harmonizing national legal approaches and international legal coordination[15]; privacy, data and consumer protection[16]; and developing countries and cybersecurity[17].

4. The first day of the meeting focused on countering spam[18] as follow-up to the ITU WSIS Thematic Meeting on Countering Spam[19], held in July 2004. This offered an opportunity to take stock of progress in countering spam initiatives, from both a technical and policy perspective, as well as to discuss possible further regional and international cooperative initiatives.

5. Approximately 150 participants took part in the meeting, representing a range of government policy-makers and regulators, international and intergovernmental organizations, privacy groups, representatives of communications service providers and ICT companies, academics, civil society organizations, and other interest groups.

****

28 June 2005 – Spam Day Sessions

Session 1: Meeting Opening and Welcome

6. Mr. Utsumi opened the meeting with a speech[20] welcoming the participants, as well as those joining the meeting via cyberspace, as it was being audiocast live over the internet and archived[21] for future reference. In his remarks, he said that at the start of the 21st century, our societies are increasingly dependent on information and communications technologies (ICTs) that span the globe. He also noted that communication networks are the lifeblood of modern societies and that

they are responsible for a growing share of national wealth, as well as providing hopes for greater prosperity. Yet, he said this dependency brings new risks. There are growing concerns that we are making ourselves increasingly vulnerable which is reinforced by a growing number of attacks in cyberspace. We are particularly worried about protecting critical infrastructures, which are systems and assets whose incapacity or destruction would have a debilitating impact on national security and the economic and social well-being of our citizens.

7. In this regard, Mr. Utsumi recalled a number of recommendations in the WSIS Plan of Action[22] that relate to building confidence and security in the use of ICTs and the promotion of a global culture of cybersecurity. Addressing cybersecurity was also recognized by the Working Group on Internet Governance[23] as a key issue that needs to be considered under the broader rubric of internet governance. He also noted this particular event was intended as a specific step toward preparing the second phase of WSIS[24] to be held in Tunis in November 2005, as well as related follow-up mechanisms after the Summit.

8. Finally, Mr. Utsumi emphasized that cyberspace does not respect national borders and no country alone can solve the world's cybersecurity problems. He said we must be creative in finding new ways to cooperate in addressing problems created by those who would abuse our networks for their own profit and gain. He further pledged that the ITU, with its broad membership of 189 Member States and over 700 private sector members, stands ready to assist in this endeavour.

9. Mr. Utsumi invited Dr. Deborah Hurley[25] to act as Chairman for the meeting, which she accepted.

10. In her opening remarks, Dr. Hurley acknowledged that there were many stakeholders in the information society represented at this meeting. She highlighted her belief that the central challenge before all of us, individually and collectively, is navigating the burgeoning sea of information. She saw the problems before us, as we look out into the near and mid-future, as not primarily technological but rather more related to economic and social policies. In particular, how do we identify our social and economic visions and leverage technologies to bring about those social and economic visions.

11. Dr. Hurley noted that today's sessions of the cybersecurity meeting would be focused on the topic of countering spam[26], with the subsequent days considering cybersecurity in a broader context. Although spam was not a problem a decade ago, it is an increasingly grave problem now. She said spam has been a fast growing tree and its roots are very wide spread, but yet its roots are shallow and that means there is an opportunity for us to fight it. She noted that there has already been some significant work on this topic as well as a good degree of international cooperation, which we would hear more about during the course of the day.

Session 2: Are We Winning or Losing the War on Spam?

12. This session[27] began with a keynote speech[28] by Steve Linford[29], Chief Executive Officer, Spamhaus[30]. In his speech, Mr. Linford set the overall tone for the day with a review of the current global situation in fighting spam. Mr. Linford said the reason we are talking about spam in the context of cybersecurity is that it is the delivery mechanism for all email security threats: phishing, endless permutations of scams, advance fee fraud, and viruses.

13. Mr. Linford noted the main exploit now used by spammers is the hijacking of millions of private computers, by infecting them with viruses, worms or trojans, turning each infected machine (viz. zombie) into an anonymous proxy under the control of the spammer. Since early 2003, almost all viruses have been created and sent out by spammers in order to build giant networks of hijacked machines through which to send their spam (viz. zombie botnets). Nowadays, over 70 per cent of spam is being sent from these hijacked computers. Spamhaus has a list of approximately four million infected machines—demonstrating the scale of the problem—with 60,000 to 100,000 new infections every week. Besides relaying spam, the other prime intent of building zombie botnets is to launch Distributed Denial of Service (DDOS)[31] attacks against internet sites.

14. Mr. Linford believes that governments do not realize how serious the threat is or that the groups behind these attacks are highly organized and criminal-minded. He said consumers are being inundated with scams, trojans, and key-loggers and, as a consequence, confidence in the internet is eroding fast. Each phishing[32] operation brings in thousands of fresh credit card and bank account numbers. The spammers have developed skills in social engineering that make emails not only appear to be from your bank, but also employ highly believable reasons for why you should trust an email and click the link. The costs of spam, including the costs of dealing with it, and of dealing with what spam delivers, such as phishing and endless financial scams is costing the world an amount we are no longer able to calculate. The cost to the financial industry alone, and to consumers, is now staggering. He concluded by noting that spam is a cancer; it is fast killing the ability to use the internet for commercial transactions and it is killing overall trust in the internet.

15. In the next presentation[33], Luc Mathan[34], representing the Messaging Anti-Abuse Working Group (MAAWG)[35], presented the experiences of messaging operators today and how MAAWG is attempting to bring the industry together to effectively address the growing problem of messaging abuse. He mentioned MAAWG's work committees, which are addressing technical, collaboration, public policy and wireless issues. MAAWG is also developing a voluntary set of principles for messaging providers directed at both members and non-members.

16. In a related presentation[36], given later during the meeting in Session 12, Mark Sunner[37], Chief Technology Officer, Messagelabs[38], highlighted their current spam, virus and zombie botnet statistics. He discussed the current sophisticated architecture for controlling zombie botnets as well as an emerging phenomenon of professional custom "malware" intended to specifically compromise internal corporate networks and steal information. He also noted that the overall attack threat will be migrating to new platforms such as mobile and Voice over Internet Protocol (VoIP) networks in the near future.

Session 3: National Policies and Legislative Approaches

17. The jurisdictional problems created by the proliferation of trans-border, unsolicited, commercial communications represent a tremendous barrier in the development of national policies, legislative approaches and, most particularly, enforcement. As spam touches on a number of aspects of law—such as commerce, advertising, criminal law, freedom of speech, and intellectual property—differences associated with the laws of the jurisdictions of the world may prove to be greater than similarities. Session 3 on National Policies and Legislative Approaches[39] to spam was chaired by Jean-Jacques Sahel[40], Assistant Director, International Communications, Department of Trade and Industry (DTI)[41], United Kingdom. This session reviewed the different approaches of national anti–spam policies and legislation around the world—as well as discussing whether harmonization is possible.

18. The first presentation[42] was a background paper commissioned by ITU, entitled A Comparative Analysis of Spam Laws: the Quest for Model Law[43] by Derek Bambauer[44], Research Fellow, Berkman Center for Internet & Society[45], Harvard Law School[46]. The goal of this paper was to help policy makers understand the potential benefits and challenges of model spam legislation as a tool to improve the security of and user confidence in information and communications technology (ICT), as well as the potential that model spam legislation holds for internet users worldwide. It analyzed the level of consensus among extant laws and the degree to which a particular component is included in most legislation and in the degree to which provisions addressing this component are similar or harmonized. The paper pointed towards zones where there is considerable consensus and illuminated the most fundamental differences, so that policymakers can tackle the hard issues and choices involved in spam laws. The paper made some preliminary recommendations for spam law efforts and considers both the potential for and the likely efficacy of a model spam law.

19. This was followed by a presentation[47] by Jonathan Kraden[48], Staff Attorney, Federal Trade Commission (FTC)[49], United States, who provided a case study of Enforcement under the US CAN-

SPAM Act: FTC v. Opt-In Global. In his concluding remarks, he said that the FTC's top priorities are: enforcement, with over 70 cases brought to date; studies on the problem of spam; consumer outreach and education; encouraging the private sector to seek solutions to the spam problem; and international cooperation in the fight against spam.

20. Miguel Montero[50], Spam Ruling Administrator, Radiografica Costarricense (RACSA)[51], Costa Rica, gave a presentation[52] on RACSA's anti-spam efforts which have dramatically reduced spam in Costa Rica, even without national spam-specific legislation. His conclusions were that Internet Service Providers (ISPs) should be accountable for the activity of their customers and that ISPs should stop all outgoing spam as soon as it is detected and known spammers and their companies should be barred from subscribing to new internet and email accounts.

21. This was followed by a presentation[53] by Liang Liu[54], Assistant Director, Anti-Spam Coordination Team, Internet Society of China[55], People's Republic of China. Mr. Liu explained the evolution of the spam situation in China, the problem of spam block lists, China's related legislation and regulation, and their Anti-Spam Coordination Team (ASCT)[56]. Mr. Liu, in his concluding remarks, noted that ASCT is in favour of setting up international coordination and cooperation with bodies like ITU, OECD, APCAUCE, FTC, IIA, IAK, IAJ, and LAP. He also said they would champion an international framework that would discuss development of effective technology solutions; provide a communication and coordinating mechanism; and facilitate free and open e-mail messaging and internet communications between Chinese ISPs and their peers in other countries.

22. In the final talk of Session 3, Maria Cristina Bueti[57], Policy Analyst, Strategy and Policy Unit, ITU, presented[58] a background paper[59] on an ITU Survey of Anti-Spam Laws and Authorities Worldwide. The survey was conducted in April 2005 and sent to ITU's 189 Member States. The survey results, based on 58 responses received, showed that there are a number of countries that have already implemented anti-spam legislation. It was shown that some countries use data protection laws or consumer protection laws to cope with spam issues. A number of countries do not have anti-spam legislation or any laws applicable to spam.

23. During this session, a review of national legislation initiatives revealed that the tools that lawmakers are using to regulate spam vary. For example, some anti-spam laws require labels or other markings to identify certain messages as unsolicited or pornographic. Others punish senders who use fraudulent or deceptive techniques (e.g., falsifying email from: addresses or using deceptive subject fields). Still others require the sender to provide his or her identity and a mechanism to remove the recipient from any future mailings. Generally, a review of national initiatives indicates a need for a combination of technical solutions, user awareness, appropriate and balanced legislation followed by measured enforcement, including industry initiatives including those in the marketing community, as well as international cooperation.

24. It was noted that developing countries are having much difficulty dealing with the problem of spam, and this often has dramatic consequences on their internet access facilities. For countries that do not have specific laws related to spam, they have had to be creative in taking other measures to deal with their specific situation. For example, in the case of Costa Rica, internet and telecommunications service providers have had to deal directly with the situation.

Session 4: International/Intergovernmental Cooperative Initiatives in Countering Spam

25. While a number of international and intergovernmental initiatives have been undertaken in the past few years, international cooperation could still be improved. Session 4 on International/Intergovernmental Cooperative Initiatives in Countering Spam[60] reviewed some of ongoing international and intergovernmental cooperative initiatives in countering spam. The session was chaired by Eric Walter[61], Chef du Bureau, Direction du Développement des Médias[62], Services du Premier Ministre, France. In an interactive panel session based on a wiki-based discussion framework[63], Mr. Walter outlined the possible national and international components of this topic and explored possible ways forward in internationally combating spam.

26. John Haydon[64], Executive Manager, Consumer and Universal Service Obligation Group, Australian Communications Authority[65], spoke of national experiences in Australia as well as giving their views on the themes and practicalities of International Anti-Spam Cooperation Initiatives[66]. Mr. Haydon noted some practicalities of international cooperation include simple and non-binding arrangements, as these are easier and more flexible than formally binding ones; information-sharing arrangements which present fewer hurdles to establishment than enforcement-cooperation arrangements; and inter-agency/working-level arrangements, which are easier than inter-governmental arrangements. Mr. Haydon noted the effectiveness of arrangements is best complemented by voluntary and informal internet operations and practices don't necessarily require legislation to be in place. He also noted that this form of cooperation can also assist in developing national anti-spam programs.

27. Philippe Gérard, Legal and Regulatory Officer, European Commission[67], spoke of a new European joint initiative entitled Contact Network of Spam Enforcement Authorities (CNSA), to combat spam through sharing information and pursuing complaints across borders in a pan-European context. During the event, he further emphasized that the five-layered approach developed at the Thematic Meeting on Countering Spam, held in July 2004, remained still valid.

28. Maneesha Mithal[68], Assistant Director, FTC's[69] International Division of Consumer Protection[70], spoke of international cooperation efforts in the London Action Plan (LAP)[71], which has a focus on international spam enforcement.

29. Tom Dale[72], General Manager, Strategic Policy Branch, Australian Department of Communications, IT & the Arts (DCITA)[73] and Chair, OECD Task Force on Spam[74] explained the Task Force continues its work on the Anti-Spam Toolkit, involving interested stakeholders as far as possible. The eight elements of the Toolkit constitute a multi-pronged and multi-stakeholder approach to the spam problem: they address regulatory and policy issues, technical solutions, enforcement concerns, and include education and awareness tools, suggestions for improved cross-border cooperation, industry best practices and outreach activities. The goal of the Toolkit is to provide useful resources and policy orientation and support to the anti-spam community. Some of this information is already available on the OECD spam website[76]. Mr. Dale emphasized that OECD endeavours to work in cooperation with APEC, ITU and other bodies to coordinate their complementary anti-spam initiatives.

30. Shamsul Jafni Shafie[77], Head, Information and Network Security Department, Monitoring and Enforcement Division, Malaysian Communications and Multimedia Commission (MCMC)[78], spoke of recent anti-spam efforts[79] in the ASEAN Telecommunications Regulators' Council (ATRC), a grouping of telecommunications regulators within the ASEAN region. During an ATRC meeting in Vientiane, Laos, in July 2004, member countries agreed for MCMC to spearhead ATRC's action plan on anti-spam. The action-plan calls for exchange of skills and information sharing; facilitating cooperation between industry and anti-spam groups within ATRC economies; bilateral agreements; and engaging in cooperation with other international groups. An ATRC meeting on countering spam[80] was held in May 2005 and further initiatives will be discussed at their next meeting in Malaysia in August 2005.

31. Augustin Ido[81], l'Institut francophone des nouvelles technologies de l'information et de la formation (Intif)[82], l'Agence intergouvernementale de la Francophonie[83] and CAPTEF[84] spoke of the particular problems that spam brings in the African and developing country context as well as their joint initiatives in French-speaking African countries to counter spam. Mr. Ido emphasized the need for increased education of computer system engineers as well as awareness raising for internet users in developing countries. He concluded his speech by putting forward the idea of having an African organization responsible for coordinating African initiatives on combating spam and cybercrime.

32. Robert Shaw[85], Internet Strategy and Policy Advisor, Strategy and Policy Unit, ITU, spoke of ITU's initiatives in countering spam which includes work in the Strategy and Policy Unit such as

the organization of the ITU WSIS Thematic Meeting on Countering Spam held in July 2004; the Telecommunications Standardization Sector, including two spam-related Resolutions adopted at the World Telecommunications Standardization Assembly in 2004 (Resolution 51 – Combating Spam[86] and Resolution 52 - Countering spam by technical means[87]); and the Telecommunication Development Sector, including anti-spam initiatives associated with the Global Symposium for Regulators[88]. He noted there was a great need for better cooperation among intergovernmental and international initiatives. He also noted it was a challenge to find a method for these different initiatives to work together and share, if not harmonize, their activities. He also mentioned discussions of aligning activities and organizing joint meetings of APEC, OECD and ITU on countering spam.

Session 5: Countering Spam: The Way Forward

33. In the final session on the countering spam day, Session 5: Countering Spam: The Way Forward[89], John Levine[90], Chair, IRTF Antispam Research Group (ASRG)[91], gave a presentation entitled The Limits of Security Technology: Lessons from the Spam Wars[92]. Echoing the comments made by the Chairman in her opening remarks (paragraph 10), he asked the audience to reflect carefully as to how technology fits in to the overall solution. He stressed that technology can be morally and politically neutral but we need to decide exactly what it is that we want. For example, an ultimate solution to spam could impact on issues such as anonymous speech, whether we wanted virtual or physical identities, or closed or open systems. These were all tradeoffs that needed to be considered.

34. A final discussion by panellists John Levine[93], Steve Linford[94], Luc Mathan[95], Jean-Jacques Sahel[96], and Eric Walter[97], moderated by the Chairman, discussed the views of each panellist's single most important ideas to most improve the countering spam situation. In this regard, a number of suggestions were made, including: promotion of the Australian legislation model and regime as a successful example of a national initiative; greater international coordination, which requires improved national coordination of relevant agencies as a prerequisite; stopping the money reward and other incentives that make spam profitable; increasing awareness and training of people about spam at all levels; finding mechanisms for governments to improve their ability to share common resources on spam; and stronger and more effective law enforcement.

35. In addition to the materials presented during the countering spam day, additional electronic contributions on national experiences were received, including: Japan Strategy to Combat Spam[98], contributed by Ministry of Internal Affairs and Communications[99], Japan; The Australian Anti-Spam Regime - A First Year Review[100], contributed by Australian Communications Authority[101], Australia; A Case Study in Enforcing AntiSpam Legislation[102] (Australia), contributed by SpamMATTERS[103]. Stopping Spam: Creating a Stronger, Safer Internet[104], contributed by Canada's Task Force on Spam[105], Canada; Brazil's CT Spam[106] (with separate presentation[107]), contributed by the Brazilian Internet Steering Committee[108] Task Force on Spam; and Mexico's Experience in Combating Spam: A Legal Perspective From a Consumer Advocate[109], contributed by Cristos Velasco, Director General, North American Consumer Project on Electronic Commerce (NACPEC)[110].

****

June 29, 2005 - Cybersecurity Sessions

Session 6: Cybersecurity Opening and Welcome

36. The Chairman, Dr. Hurley, welcomed the participants for the second day of the event and said that the following days would examine cybersecurity in a broader context. In her opening remarks, Dr. Hurley discussed the current nature of the cybersecurity problem. She noted information systems include data, information, computing devices, networks and people and that the security of information systems consists of providing for the confidentiality, integrity, availability and authentication of information and communication systems, as well as their data and information.

She said the intrinsic security of the global network of networks is growing worse every day, as more data, information, computers, networks, and, most significantly—because they represent the biggest source of risk—more fallible human beings are added. She emphasized that total cybersecurity can never be achieved but rather is an ongoing, dynamic process, particularly as it involves a learning adversary—i.e., other human beings.

37. The Chairman also emphasized that it is too narrow to take into consideration only the internet in planning for security of information systems. Instead, it is important to consider the developments surrounding convergence, which will fundamentally continue to transform how we use information and communication systems. As a result of this convergence, the internet will evolve, particularly with the deployment of Next Generation Networks (NGN)[111] and eventually to a ubiquitous information environment characterized by embeddedness, ubiquity, unboundedness and decentralization. The Chairman restated her perspective that most of the challenges related to protecting information systems are non-technical. Rather, they revolve around the management of highly complex systems, where interdependencies, magnitudes and consequences of disruptions are not yet well understood.

38. The Chairman highlighted that this meeting was being held in the context of WSIS and that from her perspective a key consideration is that the emerging global information society should be based on a sound foundation of human rights. In fact, she argued that a right to security is in itself a human right.

39. In this regard, the Chairman made references to three perhaps useful existing international regimes from which lessons might be drawn. First, there is body of several human rights conventions that have been adopted by approximately 150 countries. There is also a well-established legal and institutional framework and broad agreement on human rights principles although there has been insufficient implementation and enforcement in some countries. Second, legislation to protect personal data and privacy has been adopted in approximately 50 countries. There are also two international accords on privacy, which were adopted in the early 1980s and there is 30 years of experience in privacy legislation. Moreover, as a body of law, there is a strikingly high degree of consistency in the legal provisions for privacy and protection of personal data. Finally, there is currently a global trend to adopt legislation related to transparent access to governmental information with over 45 countries having adopted such legislation. She noted that this type of legislation, along with other government initiatives to go "online", has a corollary effect of encouraging the maintenance of robust information systems by governments.

40. Finally, Dr. Hurley put forward the notion that security of information systems must be based on five modalities: technological measures; laws; standards; norms; including both economic and social norms; and education and training. She said that it is possible that some new tools may be needed to address the challenges of information security. However, before developing these new mechanisms, it is important to review first how existing modalities and tools already can serve the information society.

Session 7: Information Sharing of National and Regional Approaches, Good Practices and Guidelines

41. Session 7: Information Sharing of National and Regional Approaches, Good Practices and Guidelines[112], chaired by Dr. Hurley, had the objective of sharing insights and strategies through examining different national and regional experiences. As background, the area of critical information infrastructure protection (CIIP) developed into a key part of national security policy during the late 1990's when a new problem became apparent: the dependency of modern industrialized societies on a wide variety of national and international information infrastructures. Since then, a number of countries began programmes to broadly address the perceived vulnerabilities of their vital information infrastructures and have proposed measures for the protection of those assets. To protect these information infrastructures and to combat cybercrime,

countries need to have procedures and systems in place for evaluating threats and vulnerabilities and preventing, responding to, and recovering from cyber incidents.

42. The session started with a presentation[113] of a background paper commissioned by ITU entitled A Comparative Analysis of Cybersecurity Initiatives Worldwide[114], prepared by Myriam Dunn[115], Head, International Relations and Security Network (ISN)[116], Center for Security Studies (CSS), Swiss Federal Institute of Technology[117], Switzerland. Her paper reviewed national cybersecurity initiatives in order to identify common themes and best practices, but especially problems and pitfalls in developing a global culture of cybersecurity. She examined how the topic of cybersecurity had made it onto the security political agenda and the characteristics of cyber-threats, including: how various governments approach the issue and their focus on common issues and problems; provided an explanation of the differences and similarities in national approaches by applying political science theory to the topic; and examined how the topic is being approached internationally.

43. In the following presentation[118], Mabito Yoshida[119], Director of IT Security Office, Information and Communications Policy Bureau, Ministry of Internal Affairs and Communications[120], Japan, presented an overview of information security policies in Japan. Mr. Yoshida described recent initiatives of the Japanese government to establish improved information security policies, including the recent establishment of a cabinet-level National Information Security Center, an Information Security Policy Council, and a National Information Security Center (NISC). Mr. Yoshida also discussed Japan's contributions to a revision of an ITU-T standard on Information Security Management[121] in the context of telecommunications. Mr. Yoshida emphasized that international cooperation is critical for information security which must be based on mutual trust among all relevant players including both government and the private sector. In that regard, he said ITU could play an invaluable role in strengthening appropriate international cooperation, for instance, by organizing fora like this meeting where all of us can exchange the latest information with one another and share the best practices to protect critical infrastructures.

Session 8: Information Sharing of National and Regional Approaches, Good Practices and Guidelines, cont'd

44. Session 8[122] provided a continuation of the theme of Session 7 and began with a presentation[123] by Pernilla Skantze[124], Policy Advisor, European Network and Information Security Agency (ENISA)[125], Belgium. She presented the status of ENISA which began operation earlier this year. She noted that in Europe, there was a recurring theme of a need to share information and raise awareness with regard to risks and best practices related to computer and internet usage. In that regard, ENISA shall help make Europeans more advanced and security conscious IT-users and they look forward to cooperating with the European network and information security community.

45. This was followed by a presentation[126] by Richard Cheong[127], Assistant Director, Infocomm Security Division, Infocomm Development Authority, Singapore. In his talk, Mr. Cheong explained that Singapore has recently adopted a three-year Infocomm Security Masterplan[128], with the goal of defending Singapore's critical infrastructure. The implementation phase of the Masterplan will now begin, with an emphasis on public-private partnerships.

46. In the final presentation of this session, Adam Golodner[129], Director, Global Security and Technology Policy, Worldwide Government Affairs, Cisco Systems Inc., focused on three broad issues in his presentation; the state of security, innovation as the key to address the security challenges and risks, and the policy implications of innovation, trust and globalization. He touched upon some of the questions related to incentives for security that had come up earlier in the meeting. His perspective was that companies have intense incentives to be secure. Security can even be seen as a competitive advantage, not only by increasing efficiency in company processes and thus productivity but it can also allow the company to build trust amongst its customers. Further, innovators are increasingly 'baking' security into architectures, moving from reactive to proactive technologies, and transitioning to self-defending networks, that can adapt to unknown threats. He

emphasized that security can be seen as a three legged stool made up of technology, processes, and people: all are needed but a balance between the three needs to be sought.

Session 9: Developing Watch, Warning and Incident Response Capabilities

47. Session 9: Developing Watch, Warning and Incident Response Capabilities[130], chaired by Suresh Ramasubramanian[131], Manager, Outblaze, India, was aimed at sharing insights and strategies in the establishment of national and regional watch, warning and incident response capabilities. This includes CSIRTs (Computer Security Incident Response Teams) and/or ISACs (Information Sharing and Analysis Centres).

48. Bing Zhang[132], Senior Engineer, CNCERT/CC, People's Republic of China, made a presentation on China's experience in building a national public network emergency response capability. In his presentation, he outlined the establishment and role of China's national CSIRT as well as their experiences and lessons learned. He concluded his talk with his perspectives on the benefits of global cooperation, including better early warning of attacks, data sharing to increase analysis capability, technical and information sharing, stopping attacks from other countries and tracing sources of attackers.

49. This was followed by a presentation by Klaus Steding-Jessen[133], Technical Manager, CERT.br, Brazil, on incident response initiatives in Brazil. He outlined the history of the establishment of CERT.br, its relationship with the Brazilian Internet Steering Committee[134], and its major initiatives. He discussed their national early warning capability which is widely distributed across the country, as is a distributed network of honeypots[135].

Session 10: Developing Watch, Warning and Incident Response Capabilities cont'd

50. Session 10[136] was a continuation of the Session 9 theme and started with a presentation by Nabil Sahli[137], Chief Executive Officer, National Agency for Computer Security, Ministry of Technologies of Communication, Tunisia. Mr. Sahli's presentation provided an overview of Tunisia's strategy in security of information systems and presentation of the CERT/Tunisian Coordination Center (TCC) services and activities. He outlined some of the particular characteristics and risks for developing economies who are at early stages of ICT development. These include a lack of awareness, lack of protection tools, and restricted availability of funds that can be devoted to cybersecurity issues. He also included some informal reflections on the particular challenges for developing economies in his presentation.

51. Through the ITU BDT cybersecurity fellowship programme, which was established to allow wider access for developing country participants to the WSIS Thematic Meeting on Cybersecurity, representatives from Least Developed Countries were given the opportunity to present the state of cybersecurity in their respective countries. For specific reference to these presentations, beginning in Session 10 and continuing subsequently throughout the event, please see paragraphs 88 and 89.

****

June 30, 2005 - Cybersecurity Sessions

Session 11: Keynote Speech by Bruce Schneier, Counterpane

52. Session 11[138] opened with a keynote speech entitled Negotiating for Security[139] (audio archive[140]) by Bruce Schneier[141], Founder and CTO, Counterpane Internet Security, Inc.[142]. Mr. Schneier started his speech by stating that security is ultimately about negotiation, explaining the title of his presentation. He stated that security is one of the fundamental building blocks of the information society as everything we now do with information requires some kind of security—sometimes a little, sometimes a lot, may it be personal, corporate or government related. He said that to a very real extent the limits of the information society can be seen as the limits of security. In other words, if we cannot do it securely, we will not do it with computers and on the internet. Therefore, this means that security is a fundamental enabling technology of the global information society. Moreover, he noted that society as a whole is increasingly moving onto computers and

networks and therefore things that had previously nothing to do with computers suddenly do: whether airplanes or the national power grid, these now have an important information security component to their secure functioning. This means that information security therefore has become our general security, which is almost everything. This fact explains our need for an increased focus on security and why the things we are trying to achieve here at this meeting are so important.

53. Mr. Schneier acknowledged that information security is not doing very well, and that computers and networks are less secure today than before—even when compared to last year. He said this is somewhat surprising as we are used to our technologies making things better, not worse. He noted that in combating spam, we are doing comparatively well. However, we still have really no idea how to systematically write secure computer programs: instead we are just trying to do our best. He also stated that every year, attacks are getting worse, and attack tools are getting more powerful and damaging. At the same time, the amount of expertise required to use attack tools is decreasing and therefore, relatively unskilled people can do lots of damage. He went further into the general topic of imbalances in security, noting that the reason why technology is scary from a security perspective is that technology can fundamentally alter security imbalances. He explained that normally there is a balance between the attacker and defender. However, technology can change this balance and make attack tools more powerful and attackers more powerful. However, sometimes technology can favour the defender. For example, the invention of the radio, which was quickly adopted by the police, altered the balance between police and criminals. But more often though, technology tends to favour the attacker because the attacker is quicker to react to it.

54. Mr. Schneier noted that all computer crime is international as on the internet you can be anywhere, and an attacker is always essentially next door to you. He continued his talk with a discussion of the issue of complexity. He stated that as a general rule, complex systems are hard to secure, and this complexity is the worse enemy of security. So even though on the internet, security is getting better, the problem is getting more complex and therefore worse faster. This is because complex systems are extremely insecure and since the internet is the most complex system every built (the telephone being the second most complex), it is no surprise that it still remains a very insecure system.

Session 12: Technical Standards and Industry Solutions

55. Session 12 on Technical Standards and Industry Solutions[143] was chaired by Bill McCrum[144], Deputy Director General, Industry Canada[145], Canada. Mr. McCrum began with an overview presentation covering ITU's standards work on Next Generation Networks (NGN)[146] as well as the foreseen security requirements. Particular targeted areas mentioned included control of spam, VoIP security, identity management, access control and authentication, data confidentiality, and secure communications. Mr. McCrum said that global collaboration was necessary, particularly in sharing network security standards information; collaboration on network security standards activities; establishing a network of security standards contacts in standards organizations; and fostering national and international databases of network security standards. Mr. McCrum cited one such national example as the US Homeland Security Standards Database[147] and an international example as ITU-T Study Group 17's[148] efforts to coordinate security standardization activities within ITU-T and beyond. Finally, he noted that network security standardization collaboration is a key element in progressing the WSIS Plan of Action[149].

56. This was followed by a presentation[150] by Arkadiy Kremer[151], Chairman, Russian Association of Networks and Services[152], Russia and Vice Chairman of ITU-T Study Group 17. Mr. Kremer discussed a standards security baseline for network operators, which is an ongoing standards project in the ITU with the objective of proposing clear criteria against which each network operator can be assessed if required. The specific usage of these criteria is dependent on the type of underlying network technology used by the operator and the related national regulatory. He concluded his talk by noting that there are a number of standards in the field of information security but these were only really standards if they widely applied. He suggested ITU could be a leader in joining together efforts of different standardization bodies on information security standardization processes.

57. The following presentation[153] of Jeffrey Sanders[154], United Nations University International Institute of Software Technology (UNU-IIST)[155] was based on a paper entitled Security and Trust for Ubiquitous Communication[156]. This paper discusses an ethical approach to security and trust in contemporary computing and communication systems and the specific consequences. The approach of the authors is that the principle of distribution should apply in which control resides as much as possible with the individual rather than in centralised agents.

58. This was followed by a presentation[157] by Mark Sunner[158], Chief Technology Officer, Messagelabs[159]. This talk is summarized in paragraph 16 above.

Session 13: Harmonizing National Legal Approaches and International Legal Coordination

59. Session 13 on Harmonizing National Legal Approaches and International Legal Coordination[160] was chaired by Dr. Hurley. This session recognizes that appropriate legislation and enforcement are two key elements in building trust in cyberspace. Yet the development of cyberspace has made a new environment for criminal offences to also become online offences. This has created problems in the application of penal legislation. As a result, many countries have made amendments in 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 current national legal approaches and areas for potential international legal coordination efforts.

60. As a start to the session, a background paper commissioned by ITU, entitled Harmonizing National Legal Approaches on Cybercrime[161], was presented by Stein Schjolberg, Chief Judge, Moss District Court[162], Norway. The paper, authored by Judge Schjolberg and Amanda Hubbard, US Department of Justice[163], provided a brief history of the issues and legislative enforcement actions taken to preserve security in cyberspace. The paper also highlighted some of the efforts regional and international groups have taken to harmonize legislation among States. It also provided background information on areas where greater standardization and harmonization work could be beneficial, particularly in the areas of legislation, criminal enforcement and judicial review. The paper argued that creating a baseline of law is desirable to ensure that no computer criminal can find a safe haven anywhere in the world. As an example, through ratifying or acceding to the Council of Europe Convention on Cybercrime[164], States agree to ensure that their domestic laws criminalize conduct described in the substantive criminal law section and establish the procedural tools necessary to investigate and prosecute such crimes. This represents a harmonizing influence of national legal approaches on cybercrime.

61. This was followed by a presentation[165] by Claudio Peguero[166], Chief, High Tech Crime Investigation Department, National Police, Dominican Republic. Mr. Peguero started his presentation by using two examples to show the possible involvement of a number of countries and different jurisdictions in single cases, as well as the need to act fast, when investigating a crime. He said that international cooperation is needed to determine the facts behind the cases in order to bring the case forward. Mr. Pequero mentioned four main areas that pose great challenges in international cooperation: enacting sufficient laws to criminalize computer abuses; committing adequate personnel and resources; improving abilities to locate and identify criminals; and improving abilities to collect and share evidence internationally to bring criminals to justice. In concluding, Mr. Peguero noted that every country relies on the others for assistance in responding to the threat of cybercrime. In that regard, he put forward the notion that each country needs to: enact adequate substantive and procedural laws; empower its law enforcement authorities to collect evidence for other countries; and work to enhance the rapid collection and international sharing of electronic evidence.

Session 14: Harmonizing National Legal Approaches and International Legal Coordination cont'd

62. Session 14[167] provided a continuation of the theme of Session 13. In the first presentation[168], Richard Downing[169], Project Overseer for Computer Crime, APEC[170], reviewed the APEC leaders' commitment to cybersecurity and the APEC Cybersecurity Strategy[171]. Mr. Downing pointed out

that ministers recognized that "the fight against cybercrime and the protection of critical infrastructure is built upon the legal frameworks of every economy". The initiatives in APEC and the work of the APEC TEL Working Group include a survey of laws in the economies, and consultations to share cybercrime legislation expertise and experience from one APEC member to another.

63. This was followed by a presentation[172] by Gianluca Esposito[173], Head, Economic Crime Section, Crime Problems Department, Council of Europe (CoE)[174]. Mr. Esposito went into detail on the Convention on Cybercrime[175] to clarify many aspects that had been brought up in the discussions earlier. He advocated for countries to adopt the Convention to explore both traditional and new methods for international cooperation. He hoped that the WSIS process would emphasize the need and desire to encourage global accession to the Convention on Cybercrime.

64. The final presentation[176] in this session was from Tony Rutkowski[177], Vice President, Regulatory Affairs, VeriSign[178], on the topic of International Cooperation for the Protection of Next Generation Network Public Infrastructure[179]. Mr. Rutkowski discussed the evolution to Next Generation Networks (NGN)[180]; issues involved in protecting public network infrastructure; the basic requirements for infrastructure protection; and the legal basis for cooperation in the prevention, operations and enforcement domains. In the area of prevention, Mr. Rutkowski highlighted the ITU's International Telecommunication Regulations (ITRs)[181], in particular Article 9.1b, of which he describes its historical context in a separate contribution entitled The ITU Treaty Provisions for Infrastructure Protection: How They Came to Be and Why They Are Relevant Today[182].

65. In his concluding remarks, Mr. Rutkowski recommended: implementing the Atlanta Declaration[183]; collaboration on NGN regulatory models and requirements, particularly those with trans-national implications; and enhancement of international institutional arrangements for protecting public NGN infrastructure. Mr. Rutkowski also highlighted a fundamental need to identify and authenticate network subscribers and providers in order to be able to protect public communication infrastructures. He said that this was the main scheme adopted[184] by the ITU to effectively protect the global public telecommunications infrastructure.

****

July 1, 2005 - Cybersecurity Sessions

Session 15: Privacy, Data and Consumer Protection

66. Session 15: Privacy, Data and Consumer Protection[185], chaired by Herbert Burkert[186], President, Research Centre for Information Law[187], University of St.Gallen, Switzerland, examined a number of initiatives to promote and codify privacy, consumer protection, and data protection rights and obligations.

67. To start the session, a presentation[188] was given by Alexander Dix[189], Berlin Commissioner for Data Protection and Freedom of Information, and Chairman of the International Working Group on Data Protection in Telecommunications (IWGDPT)[190]. Mr. Dix explained the history of IWGDPT and its context within the framework of the International Conferences on Data Protection and Privacy Commissioners. The IWGDPT has as its overall objective the improvement of privacy and data protection in telecommunications and the media. Among its other activities, the working group has proposed a series of Ten Commandments[191] to protect privacy in the internet world. Mr. Dix summarized his talk with the premise that cybersecurity is based on respect for the privacy of users; that a network under constant surveillance would create insecurity and deter users; and that there are intelligent ways to fight cybercrime and respect the human right to privacy on the internet at the same time.

68. This was followed by a presentation of a paper[192] entitled Privacy and Cyberspace: Questioning the Need for Harmonization, contributed by Gus Hosein[193], Senior Fellow, Privacy International[194]. Mr. Hosein said that we are now seeing a rise of benign 'international' standards

with a supposed compelling need to co-operate, harmonize, and standardize. He said that, as a consequence, national congresses and parliaments are no longer debating at length key issues because of their seemingly benign nature to comply with "international standards". He said that governments have learned this and are now pursuing policies internationally to establish standards that they can then bring home as benign international instruments[195]. Governments then speak of a need to harmonize as a reason to change national law, even when this may go against all prior national deliberations that may have occurred. He argued that we must stop seeing harmonization as a goal in itself. In a realm of globalised policy-making, this means that international institutions are deciding policies without scrutiny of national parliaments.

69. The next presentation[196], by Valerie Steeves[197], University of Ottawa[198], Canada, discussed the tensions between the human rights and data protection conceptions of privacy. Ms. Steeves highlighted what she saw as a fundamental disconnect between current legislative frameworks and citizen concerns about privacy. In particular, she emphasized that a focus on data protection alone cannot protect the social meaning of privacy as experienced by real people living in a community. Ms. Steeves continued her presentation with her views of the key actions that need to be taken in order to create a global culture of cybersecurity. These included: going beyond data protection as this is insufficient in itself; creating infrastructures that protect the social value of privacy as a fundamental human right; critically questioning the purposes for surveillance; and choosing the least invasive alternative so we can continue to enjoy the human right of privacy in the future.

Session 16: Developing Economies and Cybersecurity

70. Session 16: Developing Economies and Cybersecurity[199], chaired by Betty-Ellen Shave[200], Senior Counsel/Coordinator for International Computer Crime Matters[201], Department of Justice[202], United States, discussed the security issues faced by developing and transition economies and how their responses support the global cybersecurity effort.

71. A globally interconnected information network makes it clear that cybersecurity cannot be effectively addressed by individual nations or even groups of industrialized countries; it requires a combined effort by government, industry, law enforcement, and citizens of all countries worldwide. Developing countries face unique challenges in developing security policies and approaches appropriate to their circumstances. As security is an important component of the policy framework for the internet, developing countries need to: ensure that their laws cover cybercrime, develop partnerships between government and the private sector to address cybersecurity, improve the sharing of information, and raise security awareness among all users.

72. Ms. Shave highlighted that the overall US approach is to encourage the development of cybersecurity strategies, information sharing and outreach to the public. In her session remarks, she discussed a number of resources where developing countries can get assistance. To obtain assistance with drafting cybercrime statutes, examples of multilateral contacts that can be consulted include the Asia Pacific Economic Cooperation (APEC)[203], the Organization of American States (OAS)[204], and the Council of Europe (CoE)[205], as well as individual countries. Private critiques of draft cybercrime statutes can be obtained from APEC and the United States. For awareness-building or consciousness-raising, including for policy-makers; multilateral organizations such as APEC, OAS, OECD, and Interpol as well as individual states can provide good contacts. The US Department of State has also established a visitor program to aid with these kinds of initiatives. To obtain training for law enforcement in cybercrime, cyber-forensics, and how to set up a cyber-investigation unit, interested parties can consult APEC, OAS, the G8[206] (to a limited extent) and Interpol, among other multilateral groups. Moreover, many individual countries offer such training. The US provides such training via many US investigating agencies, International Law Enforcement Academies[207] on most continents, and US Agency for International Development[208] programs. In addition, developing countries themselves have valuable information to share with each other. Two other groups increasingly working in cybersecurity are the development banks (both global and regional institutions) and the private sector. There is also an increasing interest in routine formal

training of law enforcement by companies, groups of companies, national trade associations, as well as interest by the private sector in talking to national policy makers.

73. The first presentation[209] in the session was given by Michel Maechler[210], Senior ICT Specialist, World Bank[211]. Mr. Maechler noted the increased importance of ICT in development projects, whether as standalone ICT projects or as components of sectoral projects such as those in education, private sector development, government reform, agriculture, etc. He outlined some of the cybersecurity-related projects and initiatives of the World Bank. He stated that a more comprehensive cybersecurity agenda was needed including: engaging in a holistic approach to protecting critical information infrastructure; adopting multidisciplinary and cross-sectoral approaches; applying and producing practical methods and deliverables, such as country assessments; awareness raising through regional and global dialogues in conferences and workshops; dissemination of best practices and standards; building knowledge and skills; technical assistance, policy and investment lending and analytical work and surveys. Mr. Maechler also suggested three alternate ways to provide funding for cybersecurity initiatives: by raising the questions if the design and appraisal of development projects should systematically include safeguards on e-security, identification of related risks and mitigating measures; if a dedicated fund for cybersecurity should be created; and if, as many donors consider that there is enough money for ICT projects, the Digital Solidarity Fund[212] could be partly used to that effect.

74. This was followed by remarks by Sy Goodman[213], Georgia Institute of Technology[214], USA, on some of the key issues he saw facing developing economies. Mr. Goodman started his talk by noting that the growth of the internet had initially been quite slow. However, he said today the internet "comes to ground" in about 200 countries and that most of those can be described as lesser developed economies. He said that a lot had been said during the meeting emphasizing that developing economies needed to worry about cybersecurity. He saw one important new reason being the phenomenon of outsourcing. He said the basic tenet of outsourcing is that it stretches geographically the supply chain, exacerbating both problems of cybersecurity and privacy. The second issue highlighted by Mr. Goodman relates to the profile of the new kinds of users of the internet in developing economies. These are often people in rural areas who are particularly vulnerable to invasion of their privacy. Mr. Goodman also emphasized that cyber-defence at any level of skill is much harder than offence. This implies that the technical and managerial education level must be higher than that of the attackers. Yet this is a problem even in developed countries and therefore, lesser developed countries are at a huge disadvantage.

75. Mr. Goodman further emphasized what he had heard during this meeting that there was a general lack of awareness of cybersecurity issues at high levels of government. He would emphasize that this was at "especially" the highest levels in governments. Therefore, one reason he saw for lesser developed countries to become party to international agreements is that it help raised awareness at high political levels. Mr. Goodman also made a contribution to the meeting the report from a recent (May 2005) Workshop on Exploring International Dimensions of Cybersecurity[215], which co-sponsored by the Sam Nunn School of International Affairs, Georgia Tech Information Security Center, Georgia Institute of Technology, and the School of Engineering, Carnegie Mellon University.

76. The following presentation[216] by Basil Udotai[217], Coordinator, Nigerian Cybercrime Working Group (NCWG), Office of the National Security Adviser, Nigeria, began by highlighting the "development paradox of cybersecurity". The paradox is the promotion of ICT adaptation and internet penetration in developing countries while at the same time warning of the very real dangers of cybersecurity. Mr. Udotai said the internet, more than anything else before, has a great potential for redefining global cooperation. He said we must be aware of the realities of "forum shopping", which is the tendency for hackers and spammers to exploit the least regulated and most permissive jurisdictions from which to launch cyber attacks. He stated that because there is little or no incentive for security in developing economies and because it is internet connectivity, not proximity

which determines who our neighbours are on the internet, developing countries represent the weakest link on the chain of the Information Society.

77. Mr. Udotai said that evolving a truly global culture of cybersecurity means assisting developing economies in adopting the "technology, processes and people" of cybersecurity. He said that accomplishing global cybersecurity is not only essential for the survival of Information Society, but it is also a matter of strategic economic interest for advanced economies. Mr. Udotai suggested that ITU should be at the forefront of the effort to evolve a truly secure global information system. In particular, he suggested that the ITU should consider establishing a Unit to promote cybersecurity in developing economies and to harness development assistance initiatives of the advanced economies. Such a Unit would be responsible for: organizing regular meetings amongst developing economies; monitoring progress made at national levels; documenting cybersecurity measures adopted by developing economies; and coordinating experience sharing both on a peer-to-peer basis amongst developing countries and with their advanced counterparts.

78. The final speaker in this session was Alexander Ntoko[218], Chief, E-Strategies Unit, Telecommunication Development Bureau (BDT), who presented the ITU Development Sector's mandate and activities in cybersecurity. Mr. Ntoko said some of their deliverables included: implementing projects on cybersecurity for e-commerce, e-government and e-health; formulation of national policies by assisting ITU Member States in addressing technology and policy issues on IT security for e-applications and the internet; development of E-legislation through providing guidance on the development of laws and model legislation related to the prevention of cybercrime, security and data privacy and increasing awareness on secure e-applications. Mr. Ntoko also highlighted some regional cybersecurity workshops and seminars that were planned in the near future by the BDT's E-Strategies Unit[219].

Session 17: The Way Forward - Frameworks for International Cooperative Action

79. Session 17: The Way Forward – Frameworks for International Cooperative Action[220] was chaired by Deborah Hurley and looked at possible next steps and the way forward in international cooperative action.

80. As an introduction to the session, rapporteurs provided reviews of sessions held throughout the four day meeting. These rapporteurs included Tom Dale, General Manager, Strategic Policy Branch, Australian Department of Communications, IT & the Arts (DCITA) and Chair, OECD Task Force on Spam; Suresh Ramasubramanian, Manager, Outblaze, India; Bill McCrum, Deputy Director General, Industry Canada, Canada; Herbert Burkert, President, Research Centre for Information Law, University of St.Gallen, Switzerland, and Betty-Ellen Shave, Senior Counsel/Coordinator for International Computer Crime Matters, Department of Justice, United States.

81. The rapporteurs were asked by the Chairman to speak on behalf of the sessions and to give advice on the main outstanding issues that needed to be addressed in the near-, medium- and long-term. They were also asked to address the possible future role that the ITU and other international organizations could potentially play in the area of security of information systems.

82. Tom Dale, in his review of Sessions 2 through 5 on countering spam, started with a reflection on the question if we are "winning the war on spam". He said we are indeed winning some battles in preventing spam from reaching the end user. However, he saw the next battle and main issue looking forward as focusing on stopping spam being sent out in the first place. He said that key issues that needed to be addressed to reach this goal included: a common theme of focusing on international cooperation in different areas and on different levels, incorporating the needs of developing countries; the role of the private sector in cooperating with governments; the role of the regulator, the development of robust legislative tools and working together with regulators in other countries through different forums; and finally, the role of international organizations.

83. Mr. Dale noted that ITU and OECD are already in discussion on closer coordination on spam on a continuing basis and APEC is also hoped to join these discussions. It was proposed during the

meeting that APEC, OECD and ITU explore over the coming two years a series of meetings on how they could specifically rationalize their commitment of resources through sharing information on their activities and working together toward a common countering spam agenda.

84. In his intervention reviewing Sessions 9 and 10, Suresh Ramasubramanian pointed out that cybersecurity, like spam, requires two things; instant smooth and coordinated channels of communication and action, as well as split second reaction times aided by the development of new tools and monitoring systems that do not compromise user privacy. He said that acting fast and sharing information with colleagues and stakeholders around the world was crucial. However, despite all the watch and incident response systems, there are still too many users online who do not have enough awareness about the bad things that can happen to them. In order to fight the war against malware, spam, etc., a lot of hard work was still needed. He emphasized that access to secure internet resources need to be promoted and newer versions of software needs to be made readily available to everyone.

85. Bill McCrum, in reviewing Session 12, addressed some of the crucial issues important in building a robust global telecommunication platform based on standards. He spoke of the vulnerabilities that often come through quick design, and how this can ultimately hurt users in the market place. He said we should give a warning for consumers on spam: "don't buy, don't try, don't reply, and if you get scammed, don't cry" when it comes to conducting transactions on the internet today. He said that many things still needed to be done in area of standards and platforms including: standardization for the telecommunication networks and the need for international best practices and standards in the deployment of new products; guidelines to avoid products being launched with deficiencies that can easily be exploited; the need for a wider audience and participation in the standards development discussions, including the user community; the need for basic validation toolkits that can be used to assess vulnerabilities in new technologies that are about to be deployed in a telecommunication network; and finally, the need for focused attention on formal techniques for communication protocols. He concluded with the remark that on the internet everyone is your neighbour, and there are some pretty shady neighbours out there.

86. Herbert Burkert looked at the issues discussed in Session 15 through a number of micro, meso, and macro level suggestions. On the micro level, these included the exchange of best practices to encourage human rights-enhancing cybersecurity systems; exchange programmes for personnel from the security side and human rights organizations; and encouraging people to assess their own cyber behaviour on a more regular basis. On the meso level, he said that there was a need for a shift from a security guided approach to a risk oriented approach; encouraging more risk assessment, risk education, risk communication, and risk insurance as well as the reconsideration of the keyword "trust". On the macro level, he said two additional values should be added to the risk equation; "privacy" as a prerequisite to reach any other as a human right, and "transparency". In conclusion, he emphasized that stakeholders need to look for new platforms that allowed for international organizations to share and exchange their findings, set up standards, and norms.

87. Betty-Ellen Shave, in reviewing Session 16, discussed the United States of America's approach to encouraging the development of national cybersecurity strategies. She said the elements of such strategies could include: adequate legal frameworks; watch, warning and recovery efforts; public-private partnerships; and outreach to the public to build a culture of cybersecurity. Within this framework, Ms. Shave encouraged that ITU should consider which elements of this strategy lies within the ITU's mandate as determined by its Member States.

Additional Contributions to the Event

88. Through the ITU BDT cybersecurity fellowship programme, which was established to allow wider access for developing country participants to the WSIS Thematic Meeting on Cybersecurity, representatives from Least Developed Countries were given the opportunity to present the state of cybersecurity in their respective countries. These presentations included: State of Cybersecurity in Afghanistan, contributed and presented by Khaled Saleem, Ministry of Communications,

Afghanistan; Cyber Security - Bangladesh Perspective, contributed by Reza Salim, Bangladesh Friendship Education Society (BFES), Bangladesh; State of Cyber Security in Ethiopia, contributed and presented by Balcha Reba, Ethiopian Telecommunication Agency, Ethiopia; State of Cybersecurity in Lao PDR, contributed by Somlouay Kittignavong, Science Technology and Environment Agency (STEA) and presented by Khamla Sounnalat, Ministry of Communications, Transports, Posts & Constructions, People's Democratic Republic of Lao; State of Cyber Security in Lesotho, contributed and presented by Ntabiseny Pule, Lesotho Telecommunications Authority, Lesotho; Country Paper: Maldives, contributed and presented by Naheed Mohamed Riza, National Centre for Information Technology, Maldives; Cybersecurity in Context of Nepal, contributed and presented by Laxmi Kanta Shrestha, Nepal Telecom, Nepal; Reunion Thematic du SMSI sur la Cyber securite - Contribution du Niger , contributed by Aboubacar Abdou Fogue, Ministère de la Communication, Niger; Cyber Security in Tanzania - Country Report, contributed and presented by Peter Rudolf Ulanga, Tanzania; State of Cybersecurity in Uganda, contributed and presented by Simon Bugaba, Uganda Communications Commission, Uganda; and State of Cybersecurity in Zambia, contributed and presented by Patrick Mubanga Mutimushi, Communications Authority, Zambia.

89. These speakers provided valuable insights into the cybersecurity challenges in their countries, demonstrating how lack of awareness, coordination, information sharing and trained human resources are challenges. It was pointed out that as laws often take very long to put in place and must also be matched by effective enforcement, other complementary measures need to be taken immediately to be able to work towards a more secure cyberspace. Often lacking in resources, developing countries representatives learned that cybersecurity is an issue of concern in both developing and developed countries, and hopefully this mean that solutions will be sought on a global scale.

90. In addition to the background papers presented in the different sessions, and the contributions received through the ITU BDT fellowship programme discussed in paragraphs 88 and 89, additional contributions to the event were received. These included: Legal Framework for Ensuring Cybersecurity in the Republic of Azerbaijan, contributed by Ministry of Communications and Information Technologies, Republic of Azerbaijan; Creating a Safer Information Society - National Information Security Strategy, contributed by the National Information Security Advisory Board, Finland; Vers l'Etablissement d'une Souverainete Nationale Numerique, contributed by Organisation Internationale pour la Sécurité des Transactions Electroniques (OISTE) and WISeKey SA; La Société de l'Information et les Problèmes de Sécurité, contributed by J. Archibald of McGill University; Workshop on Exploring International Dimensions of Cybersecurity, contributed by Carnegie Mellon University; The ITU Treaty Provisions for Infrastructure Protection: How They Came to Be and Why They Are Relevant Today, contributed by Anthony Rutkowski; and Privacy and Cyberspace: Questioning the Need for Harmonization, contributed and presented by Gus Hosein, Privacy International.

Session 18: Close of Meeting and Summary

91. In her remarks both during and in summarizing the event, Dr. Hurley put forward a number of comments and reflections on the WSIS Thematic Meeting on Cybersecurity.

92. With regard to the first day's discussion on spam, valuable experiences had been gained since the ITU WSIS Thematic Meeting on Countering Spam held in July 2004. However, there was no clear consensus as to whether we were winning or losing the war on spam. Complicating this was that spam was under constant mutation from an annoyance to a more general cybersecurity threat. Spam should also be seen as not limited to internet email but rather considered in a broader context of "unwanted or unsolicited communications". As examples, experts said spam is very likely to migrate in the near future to new platforms such as mobile and Voice over Internet Protocol (VoIP) networks. Spam was also seen as increasingly a professional criminal activity and a delivery mechanism for many other security threats including phishing, endless permutations of scams,

advance fee fraud, and viruses. A consequence of this was that studies demonstrated that consumer confidence in the internet was eroding fast[221].

93. Spammers are now more effectively leveraging the hijacking of millions of private computers, by infecting them with viruses, worms or trojans, turning each infected machine (viz. zombie) into an anonymous proxy under the control of the spammer. These zombie botnets, besides relaying spam, were also being used to launch Distributed Denial of Service (DDOS)[222] attacks against internet sites.

94. The WSIS Thematic Meeting on Countering Spam, held in July 2004, suggested that a comprehensive approach to countering spam should be five-layered, including:

- Strong legislation;
- The development of technical measures;
- The establishment of industry partnerships, especially with Internet Service Providers, mobile carriers and direct marketing associations;
- The education of consumers and industry players about anti-spam measures and Internet security practices;
- International cooperation at the levels of government, industry, consumer, business and anti-spam groups, to allow a global and coordinated approach to the problem.

Evolution in each of the areas is discussed below.

95. **Strong legislation:** On the legislative front, a great deal of experience has also been gained as to the commonality, differences and effectiveness of different approaches of national anti-spam legislation. A background paper entitled A Comparative Analysis of Spam Laws: the Quest for Model Law[223] analyzed the level of consensus and differences among extant laws and made some preliminary recommendations for inclusion in national spam legislation. It also considered the potential for and the likely efficacy of a model spam law. However, it was also emphasized by a number of speakers that as spam has become a more criminal-like activity, legislation was not particularly helpful unless it was tied to effective enforcement. This enforcement is often expensive, complex, and cross-jurisdictional in nature which has lead to several international initiatives focused on cross-border enforcement[224].

96. **The development of technical measures:** On the technical measures front, although there has been a lot of related activity, no single standard had yet emerged from a number of proposals (e.g., SPF[225], Sender ID[226], DKIM[227], CSV[228], CLEAR[229]). In fact, it was emphasized that these technical proposals do not directly stop spam—rather they provide a mechanism to authenticate the sender thus preventing the spammer's server from masquerading as another source.

97. **The establishment of industry partnerships, especially with Internet Service Providers, mobile carriers and direct marketing associations:** One new development is that a number of messaging operators have established the Messaging Anti-Abuse Working Group (MAAWG)[230], bringing the industry together to effectively address the growing problem of messaging abuse on both technical and policy fronts. MAAWG is active in evaluating different anti-spam technologies from a provider's point of view[231].

98. **The education of consumers and industry players about anti-spam measures and Internet security practices:** It was clear that there was a significant need to raise awareness of the need for a systematic and consistent approach to spam and more general cybersecurity issues and to promote user education and training. A programme of education and training needs to be developed at all levels, including for schoolchildren, in order to reinforce an understanding of security issues, as well as discouraging teenagers from becoming hackers. Security should also become a component of information system design courses, for example, by ensuring the systematic inclusion of security considerations during design projects.

99. **International cooperation at the levels of government, industry, consumer, business and anti-spam groups, to allow a global and coordinated approach to the problem:** Much work still needs to be done on international countering spam cooperation involving many actors. At the simplest level, this implies sharing information on the many disparate activities taking place. At that next level, this means attempting to rationalize activities through joint cooperation projects. There are a number of international cooperation initiatives[232] underway. At the intergovernmental level, APEC, OECD and ITU are beginning to explore through a series of meetings how they could rationalize their commitment of resources through sharing information on their activities and work together toward a common countering spam agenda. There are also a growing number of national and regional initiatives to educate users on how to safely use the internet. The rapid recent increase in phishing and identity theft, widely reported in the press, has also served to sensitize users.

100. On the broader issues of **cybersecurity**, the Chairman restated her perspective that most of the challenges related to protecting information systems are non-technical. Rather, they revolve around the management of highly complex systems, where interdependencies, magnitudes and consequences of disruptions are not yet well understood. This was echoed by other speakers. For example, Bruce Schneier in his talk noted that complex systems are hard to secure, and therefore complexity is the worse enemy of security. So while internet security is getting better, the total environment is growing in complexity and as a result overall security is getting worse. There are a number of factors that contribute to this, including the continual addition of more computers, communication networks, data, information, and, most significantly, human beings. In the latter case, it was demonstrated[233] by Mr. Schneier that there is an inverse relationship between the availability of hacking tools on the World Wide Web and the necessary sophistication of hackers. Therefore, less and less skill is needed to do damage. He noted that security is never an abstract concept; it is always in context of an attacker and a defender. In the WSIS process, it is vital to remember whose interests we are serving: governments', businessess', or the peoples'. Cybercrime and cyberterrorism is important, and there are many international bodies already working on those problems. Where the WSIS can make a difference is in cyber-rights: security from government and business. As more of our society extends into cyberspace, it is vital that the international community demand that governments and businesses respect human rights in cyberspace, privacy in cyberspace, and fair-use rights in cyberspace. The very aspects of computers that make crime such a problem also makes it easy for powerful organizations to trample individual rights.

101. Despite the insecurity of the internet, it was also clear that the performance criteria and quality of service requirements expected of the internet were changing rapidly, as it becomes a mass medium used widely throughout society. The early internet performance standard was “best effort”. It is apparent from ongoing convergence that this quality of service performance and guarantee is no longer sufficient and that a standard similar to that applied to telephony services and emergency services—i.e., constant availability—will be required. It was noted that many of these considerations are being debated under the context of architectural and security considerations of standards for Next Generation Networks.

102. It was repeatedly noted during the event that while a lot is known about computer security, implementation lags far behind, with continued failure to implement security measures. There are a number of reasons for this. To date, reliable data and indicators on security vulnerabilities, threats, and breaches is still insufficient. It is argued that better data will help because it will demonstrate more clearly the need for improved information security. Likewise, incentive structures to encourage individuals and the private sector to improve critical infrastructure protection may be necessary. This could take the form of insurance requirements, liability, standards, deductions and/or tax credits.

103. Dr. Hurley noted an issue that had been raised was more consideration as to the potential liability of software developers for bugs in their products and services. However, it was also put forward that companies now have sufficient incentives to be secure and build secure products. In that regard, security could be seen as a competitive advantage, not only by increasing efficiency in

company processes and thus productivity but because it allows the company to build trust amongst its customers.

104. As the internet evolves into a public infrastructure necessary for the general functioning of society, there are new considerations evolving for protection of this critical infrastructure. It can be noted that governments typically impose certain capability requirements when the general public is dependent on an infrastructure. Therefore, security includes not only the important issue of robust performance for daily business and personal activities, but also inevitably raises issues of critical infrastructure protection, law enforcement and national security. The background paper entitled A Comparative Analysis of Cybersecurity Initiatives Worldwide[234], provided insights into common themes and best practices by different countries; how the topic of cybersecurity had made it onto the security political agenda, and how the topic is being approached internationally.

105. The background paper entitled Harmonizing National Legal Approaches on Cybercrime[235] provide a history of the issues and highlights some of the efforts regional and international groups have taken to harmonize legislation. The paper also suggests areas where additional work could be beneficial, particularly related to legislation, criminal enforcement and judicial review. Generally, it was felt that creating a baseline of law globally is desirable to ensure that no computer criminal can find a safe haven. There remain a number of challenges in this area including enacting sufficient laws to criminalize computer abuses; committing adequate personnel and resources; improving abilities to locate and identify criminals; and improving abilities to collect and share evidence internationally to bring criminals to justice.

106. The Chairman stated that while law enforcement and national security issues must be competently addressed, they must be accomplished based on a foundation of human rights and in the context of the use of these information systems in civil society. In that regard, she pointed out that there is a body of several human rights conventions that have been adopted by approximately 150 countries.

107. There was debate about the tensions between security, human rights and data protection. It was stated by speakers that a focus on data protection alone cannot protect our social meaning of privacy as experienced by real people living in a community. In this regard, privacy and security should be seen as compatible and mutually reinforcing. Indeed a right to security could be considered itself as a human right and it was expressed that we should chose the least invasive alternative so we can continue to enjoy the human right of privacy in the future.

108. Evolving a global culture of cybersecurity also means assisting developing economies in adopting the "technology, processes and people" of cybersecurity. Developing countries had a particular set of challenges, including lack of awareness (particularly at high levels of government), coordination, information sharing and trained human resources. Highlighted was the "development paradox of cybersecurity" where there is promotion of ICT adaptation and internet penetration in developing countries while at the same time warning of the very real dangers of cybersecurity.

109. It was noted that trained cybersecurity professional are lacking even in developed countries so developing economies are at a huge disadvantage. Often lacking in resources and with little or no incentives to address these issues, developing countries represent the weakest link on the chain of the Information Society. It was also stated that the new users on the internet from developing economies were particularly vulnerable.

110. In the context of developing countries, it was stated several times during the event that the adoption or recognition of base-related legislation could help facilitate international cooperation to combat cybersecurity threats and that this also assisted in raising awareness at high national political levels. However, it was also argued that this international harmonization should be balanced against national due legislative process. Equally, exchanges of best practices among developing countries should be encouraged. Learning from other national experience, countries could establish a balanced national security policy framework and adequate monitoring tools; adopt or recognize base standards for e-security for government agencies; create CERT/CISRT type

activities; create an e-security culture through awareness programs and capacity building; and promote private sector and public/private sector initiatives.

111. In the international arena, more linkages and coordination are clearly needed between all stakeholders. While there is urgency in tackling cybersecurity issues, there is also a need for pragmatic simple steps towards international cooperation and capacity building from current national experiences through an inclusive dialogue involving all actors and international organizations that have a role and expertise in cybersecurity issues. A necessary next step involves identifying the specific roles of different stakeholders relative to the themes addressed in this event including: information sharing of national and regional approaches, good practices and guidelines[236]; developing watch, warning and incident response capabilities[237]; technical standards and industry solutions[238]; harmonizing national legal approaches and international legal coordination[239]; privacy, data and consumer protection[240]; and developing countries and cybersecurity[241].

112. The Chairman said that as this particular event was held in the context of preparation for the second phase of WSIS[242], to be held in Tunis in November 2005, and related follow-up mechanisms, the results of this meeting will therefore be reported to the WSIS preparatory process.

113. In closing the meeting, the Chairman thanked the participants, the ITU Secretary-General and all involved ITU staff for their efficient and dedicated support for this event.

---

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

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

[3] http://www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=1161|1160

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

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

[6] http://www.itu.int/osg/spu/cybersecurity/agenda.pdf

[7] http://www.itu.int/osg/spu/cybersecurity/material.html

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

[9] http://www.itu.int/osg/spu/cybersecurity/material.html

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

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

[12] http://www.itu.int/osg/spu/cybersecurity/agenda.html#session7

[13] http://www.itu.int/osg/spu/cybersecurity/agenda.html#session9

[14] http://www.itu.int/osg/spu/cybersecurity/agenda.html#session12

[15] http://www.itu.int/osg/spu/cybersecurity/agenda.html#session13

[16] http://www.itu.int/osg/spu/cybersecurity/agenda.html#session15

[17] http://www.itu.int/osg/spu/cybersecurity/agenda.html#session16

[18] http://www.itu.int/osg/spu/cybersecurity/agenda.html#session2

[19] http://www.itu.int/osg/spu/spam/index.phtml

[20] http://www.itu.int/osg/spu/cybersecurity/presentations/cybersecurity-utsumi-opening.pdf

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

[22] http://www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=1161|1160

[23] http://www.wgig.org

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

[25] http://www.itu.int/osg/spu/cybersecurity/speaker_bios.html#hurley

[26] http://www.itu.int/osg/spu/cybersecurity/agenda.html#session2

[27] http://www.itu.int/osg/spu/cybersecurity/agenda.html#session2

[28] http://www.itu.int/osg/spu/cybersecurity/presentations/keynote-linford-spamhaus.pdf

[29] http://www.itu.int/osg/spu/cybersecurity/speaker_bios.html#linford

[30] http://www.spamhaus.org

[31] See http://staff.washington.edu/dittrich/misc/ddos/ for references on DDOS.

[32] See http://www.antiphishing.org/ for an explanation of phishing.

[33] http://www.itu.int/osg/spu/cybersecurity/presentations/session2_mathan.pdf

[34] http://www.itu.int/osg/spu/cybersecurity/speaker_bios.html#mathan

[35] http://www.maawg.org

[36] http://www.itu.int/osg/spu/cybersecurity/presentations/session12_sunner.pdf

[37] http://www.itu.int/osg/spu/cybersecurity/speaker_bios.html#sunner

[38] http://www.messagelabs.com/

[39] http://www.itu.int/osg/spu/cybersecurity/agenda.html#session3

[40] http://www.itu.int/osg/spu/cybersecurity/speaker_bios.html#sahel

[41] http://www.dti.gov.uk/

[42] http://www.itu.int/osg/spu/cybersecurity/presentations/session3_bambauer.pdf

[43] See http://www.itu.int/osg/spu/cybersecurity/docs/Background_Paper_Comparative_Analysis_of_Spam_Laws.pdf. The authors of the paper are Derek E. Bambauer, John G. Palfrey, Jr., and David E. Abrams, Berkman Center for Internet & Society, Harvard Law School.

[44] http://www.itu.int/osg/spu/cybersecurity/speaker_bios.html#bambauer

[45] http://cyber.law.harvard.edu/home/

[46] http://www.law.harvard.edu/

[47] http://www.itu.int/osg/spu/cybersecurity/presentations/session3_kraden.pdf

[48] http://www.itu.int/osg/spu/cybersecurity/speaker_bios.html#kraden

[49] http://www.ftc.gov/

[50] http://www.itu.int/osg/spu/cybersecurity/speaker_bios.html#montero

[51] http://www.racsa.co.cr/

[52] http://www.itu.int/osg/spu/cybersecurity/presentations/session3_montero.pdf

[53] http://www.itu.int/osg/spu/cybersecurity/presentations/session3_liu.pdf

[54] http://www.itu.int/osg/spu/cybersecurity/speaker_bios.html#liu

[55] http://www.isc.org.cn

[56] http://www.spam.com.cn/

[57] http://www.itu.int/osg/spu/cybersecurity/speaker_bios.html#bueti

[58] http://www.itu.int/osg/spu/cybersecurity/presentations/session3_bueti.pdf

[59] http://www.itu.int/osg/spu/cybersecurity/docs/Background_Paper_ITU_Bueti_Survey.pdf

[60] http://www.itu.int/osg/spu/cybersecurity/agenda.html#session4

[61] http://www.itu.int/osg/spu/cybersecurity/speaker_bios.html#walter

[62] http://www.ddm.gouv.fr/

[63] http://spam.e-soc.org/wiki/index.php/Spam_ITU_en

[64] http://www.itu.int/osg/spu/cybersecurity/speaker_bios.html#haydon

[65] http://www.acma.gov.au/

[66] http://www.itu.int/osg/spu/cybersecurity/presentations/session4_haydon.pdf

[67] http://europa.eu.int/comm/index_en.htm

[68] http://www.itu.int/osg/spu/cybersecurity/speaker_bios.html#mithal

[69] http://www.ftc.gov/

[70] http://www.ftc.gov/bcp/bcpidcp.htm

[71] http://www.ftc.gov/os/2004/10/041012londonactionplan.pdf

[72] http://www.itu.int/osg/spu/cybersecurity/speaker_bios.html#dale

[73] http://www.dcita.gov.au/

[74] www.oecd.org/sti/spam/

[75] http://www.oecd.org/sti/spam/toolkit

[76] http://www.oecd.org/sti/spam/

[77] http://www.itu.int/osg/spu/cybersecurity/speaker_bios.html#jafni

[78] http://www.mcmc.gov.my/

[79] http://www.itu.int/osg/spu/cybersecurity/presentations/session4_jafnie.pdf

[80] http://www.mcmc.gov.my/what_we_do/ins/ATRC/Final%20Program.pdf

[81] http://www.itu.int/osg/spu/cybersecurity/speaker_bios.html#ido

[82] http://intif.francophonie.org/

[83] http://agence.francophonie.org/agence/index.cfm

[84] http://www.telecom.gouv.fr/international/captef/body.htm

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

[86] http://www.itu.int/ITU-T/wtsa/resolutions04/Res51E.pdf

[87] http://www.itu.int/ITU-T/wtsa/resolutions04/Res52E.pdf

[88] http://www.itu.int/ITU-D/treg/

[89] http://www.itu.int/osg/spu/cybersecurity/agenda.html#session5

[90] http://www.itu.int/osg/spu/cybersecurity/speaker_bios.html#levine

[91] http://asrg.sp.am/

[92] http://www.itu.int/osg/spu/cybersecurity/presentations/session5_levine.pdf

[93] http://www.itu.int/osg/spu/cybersecurity/speaker_bios.html#levine

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

[95] http://www.itu.int/osg/spu/cybersecurity/speaker_bios.html#mathan

[96] http://www.itu.int/osg/spu/cybersecurity/speaker_bios.html#sahel
[97] http://www.itu.int/osg/spu/cybersecurity/speaker_bios.html#walter
[98] http://www.itu.int/osg/spu/cybersecurity/contributions/Japan_contribution.pdf
[99] http://www.soumu.go.jp/index.html
[100] http://www.itu.int/osg/spu/cybersecurity/contributions/Australia_spamregime_review.pdf
[101] http://www.acma.gov.au/
[102] http://www.itu.int/osg/spu/cybersecurity/contributions/SpamMATTERS_contribution.pdf
[103] http://www.spammatters.com/
[104] http://www.itu.int/osg/spu/cybersecurity/docs/Canada_stopping_spam.pdf
[105] http://e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/en/h_gv00248e.html
[106] http://www.itu.int/osg/spu/cybersecurity/contributions/Brazilian_antispam_taskforce_contribution.pdf
[107] http://www.itu.int/osg/spu/cybersecurity/contributions/Brazilian_antispam_taskforce_presentation.pdf
[108] http://www.cgi.br/
[109] http://www.itu.int/osg/spu/cybersecurity/contributions/Mexico_contribution.pdf
[110] http://www.nacpec.org
[111] http://www.itu.int/osg/spu/ngn/
[112] http://www.itu.int/osg/spu/cybersecurity/agenda.html#session7
[113] http://www.itu.int/osg/spu/cybersecurity/presentations/session7_dunn.pdf
[114] http://www.itu.int/osg/spu/cybersecurity/docs/Background_Paper_Comparative_Analysis_Cybersecurity_Initiatives_Worldwide.pdf
[115] http://www.itu.int/osg/spu/cybersecurity/speaker_bios.html#dunn
[116] http://www.isn.ethz.ch/
[117] http://www.ethz.ch/
[118] http://www.itu.int/osg/spu/cybersecurity/presentations/session7_yoshida.pdf
[119] http://www.itu.int/osg/spu/cybersecurity/speaker_bios.html#yoshida
[120] http://www.soumu.go.jp/index.html
[121] http://www.itu.int/rec/recommendation.asp?type=folders&lang=e&parent=T-REC-X.1051
[122] http://www.itu.int/osg/spu/cybersecurity/agenda.html#session8
[123] http://www.itu.int/osg/spu/cybersecurity/presentations/session8_skantze.pdf
[124] http://www.itu.int/osg/spu/cybersecurity/speaker_bios.html#skantze
[125] http://www.enisa.eu.int/
[126] http://www.itu.int/osg/spu/cybersecurity/presentations/session8_cheong.pdf
[127] http://www.itu.int/osg/spu/cybersecurity/speaker_bios.html#cheong
[128] http://www.ida.gov.sg/idaweb/media/infopage.jsp?infopagecategory=infocommsecurity.mr:media&versionid=3&infopageid=I3280
[129] http://www.itu.int/osg/spu/cybersecurity/speaker_bios.html#golodner
[130] http://www.itu.int/osg/spu/cybersecurity/agenda.html#session9
[131] http://www.itu.int/osg/spu/cybersecurity/speaker_bios.html#ramasubramanian
[132] http://www.itu.int/osg/spu/cybersecurity/speaker_bios.html#zhang
[133] http://www.itu.int/osg/spu/cybersecurity/speaker_bios.html#steding-jessen
[134] http://www.cgi.br/
[135] http://www.honeynet.org/papers/individual/
[136] http://www.itu.int/osg/spu/cybersecurity/agenda.html#session10
[137] http://www.itu.int/osg/spu/cybersecurity/speaker_bios.html#sahli
[138] http://www.itu.int/osg/spu/cybersecurity/agenda.html#session11
[139] http://www.itu.int/osg/spu/cybersecurity/presentations/session11_schneier.pdf
[140] http://www.itu.int/ibs/sg/spu/cybersecurity/Links/B-20050630-0930-en.smil
[141] http://www.itu.int/osg/spu/cybersecurity/speaker_bios.html#schneier
[142] http://www.counterpane.com
[143] http://www.itu.int/osg/spu/cybersecurity/agenda.html#session12
[144] http://www.itu.int/osg/spu/cybersecurity/speaker_bios.html#mccrum
[145] http://www.ic.gc.ca/
[146] http://www.itu.int/osg/spu/ngn/
[147] http://www.hssd.us/
[148] http://www.itu.int/ITU-T/studygroups/com17/index.asp
[149] http://www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=1161|1160
[150] http://www.itu.int/osg/spu/cybersecurity/presentations/session12_kremer.pdf
[151] http://www.itu.int/osg/spu/cybersecurity/speaker_bios.html#kremer
[152] http://www.rans.ru/
[153] http://www.itu.int/osg/spu/cybersecurity/presentations/session12_sanders.pdf
[154] http://www.itu.int/osg/spu/cybersecurity/speaker_bios.html#sanders

[155] http://www.iist.unu.edu/

[156] http://www.itu.int/osg/spu/cybersecurity/contributions/UNU-IIST_contribution.pdf

[157] http://www.itu.int/osg/spu/cybersecurity/presentations/session12_sunner.pdf

[158] http://www.itu.int/osg/spu/cybersecurity/speaker_bios.html#sunner

[159] http://www.messagelabs.com/

[160] http://www.itu.int/osg/spu/cybersecurity/agenda.html#session13

[161] See http://www.itu.int/osg/spu/cybersecurity/docs/Background_Paper_Harmonizing_National_and_Legal_Approaches_on_Cybercrime.pdf. The authors of the paper are Stein Schjolberg, Chief Judge, Moss District Court, Norway and Amanda Hubbard, Trial Attorney, Computer Crime and Intellectual Property Division US Department of Justice, United States.

[162] http://www.mosstingrett.no/

[163] http://www.usdoj.gov/

[164] http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CM=7&DF=08/07/2005&CL=ENG

[165] http://www.itu.int/osg/spu/cybersecurity/presentations/session13_peguero.pdf

[166] http://www.itu.int/osg/spu/cybersecurity/speaker_bios.html#pequero

[167] http://www.itu.int/osg/spu/cybersecurity/agenda.html#session14

[168] http://www.itu.int/osg/spu/cybersecurity/presentations/session14_downing.pdf

[169] http://www.itu.int/osg/spu/cybersecurity/speaker_bios.html#downing

[170] http://www.apec.org/

[171] http://www.apectelwg.org/e-securityTG/index.htm

[172] http://www.itu.int/osg/spu/cybersecurity/presentations/session14_esposito.pdf

[173] http://www.itu.int/osg/spu/cybersecurity/speaker_bios.html#esposito

[174] http://www.coe.int

[175] http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CM=7&DF=08/07/2005&CL=ENG

[176] http://www.itu.int/osg/spu/cybersecurity/presentations/session14_rutkowski.pdf

[177] http://www.itu.int/osg/spu/cybersecurity/speaker_bios.html#rutkowski

[178] http://www.verisign.com/

[179] http://www.itu.int/osg/spu/cybersecurity/presentations/session14_rutkowski.pdf

[180] http://www.itu.int/osg/spu/ngn/

[181] http://www.itu.int/ITU-T/itr/index.html

[182] http://www.itu.int/osg/spu/cybersecurity/contributions/Rutkowski_contribution.pdf

[183] See http://www.itu.int/osg/spu/cybersecurity/contributions/Carnegie_Mellon_Atlanta_contribution.pdf, Workshop on Exploring International Dimensions of Cybersecurity.

[184] See ITU Carrier Codes defined in ITU-T Recommendation M.1400 at http://www.itu.int/ITU-T/inr/icc/.

[185] http://www.itu.int/osg/spu/cybersecurity/agenda.html#session15

[186] http://www.itu.int/osg/spu/cybersecurity/speaker_bios.html#burkert

[187] http://www.fir.unisg.ch/org/fir/web.nsf/wwwPubhomepage/webhomepageeng?opendocument

[188] http://www.itu.int/osg/spu/cybersecurity/presentations/session15_dix.pdf

[189] http://www.itu.int/osg/spu/cybersecurity/speaker_bios.html#dix

[190] http://www.datenschutz-berlin.de/doc/int/iwgdpt/

[191] http://www.datenschutz-berlin.de/doc/int/iwgdpt/tc_en.htm

[192] http://www.itu.int/osg/spu/cybersecurity/docs/Hosein_Privacy_and_Cyberspace.pdf

[193] http://www.itu.int/osg/spu/cybersecurity/speaker_bios.html#hosein

[194] http://www.privacyinternational.org/

[195] This is sometimes called 'policy laundering'. For example, see http://www.policylaundering.org/.

[196] http://www.itu.int/osg/spu/cybersecurity/presentations/session15_steeves.pdf

[197] http://www.itu.int/osg/spu/cybersecurity/speaker_bios.html#steeves

[198] http://www.uottawa.ca/

[199] http://www.itu.int/osg/spu/cybersecurity/agenda.html#session16

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

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

[202] http://www.usdoj.gov/

[203] http://www.apec.org/

[204] http://www.oas.org/

[205] http://www.coe.int/

[206] http://en.wikipedia.org/wiki/G8

[207] http://www.state.gov/g/inl/ilea/

[208] http://www.usaid.gov/

[209] http://www.itu.int/osg/spu/cybersecurity/presentations/session16_maechler.pdf

[210] http://www.itu.int/osg/spu/cybersecurity/speaker_bios.html#maechler

[211] http://www.worldbank.int/

[212] http://www.dsf-fsn.org/

[213] http://www.itu.int/osg/spu/cybersecurity/speaker_bios.html#goodman

[214] http://www.gatech.edu/

[215] http://www.itu.int/osg/spu/cybersecurity/contributions/Carnegie_Mellon_Atlanta_contribution.pdf

[216] http://www.itu.int/osg/spu/cybersecurity/presentations/session16_udotai.pdf

[217] http://www.itu.int/osg/spu/cybersecurity/speaker_bios.html#udotai

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

[219] http://www.itu.int/ITU-D/e-strategy/

[220] http://www.itu.int/osg/spu/cybersecurity/agenda.html#session17

[221] For example, see http://www.pewinternet.org/report_display.asp?r=102 and http://www.gartner.com/press_releases/asset_129754_11.html

[222] See http://staff.washington.edu/dittrich/misc/ddos/ for references on DDOS.

[223] See http://www.itu.int/osg/spu/cybersecurity/docs/Background_Paper_Comparative_Analysis_of_Spam_Laws.pdf. The authors of the paper are Derek E. Bambauer, John G. Palfrey, Jr., and David E. Abrams, Berkman Center for Internet & Society, Harvard Law School.

[224] http://www.itu.int/osg/spu/spam/intcoop.html

[225] http://spf.pobox.com/

[226] http://www.microsoft.com/mscorp/safety/technologies/senderid/

[227] http://mipassoc.org/mass/

[228] http://mipassoc.org/csv/

[229] http://mipassoc.org/clear/

[230] http://www.maawg.org

[231] For example, see http://www.maawg.org/news/maawg050711 on its evaluation of email authentication proposals.

[232] For example, see http://www.itu.int/osg/spu/spam/intcoop.html

[233] http://www.itu.int/osg/spu/cybersecurity/presentations/session11_schneier.pdf

[234] http://www.itu.int/osg/spu/cybersecurity/docs/Background_Paper_Comparative_Analysis_Cybersecurity_Initiatives_Worldwide.pdf

[235] See http://www.itu.int/osg/spu/cybersecurity/docs/Background_Paper_Harmonizing_National_and_Legal_Approaches_on_Cybercrime.pdf. The authors of the paper are Stein Schjolberg, Chief Judge, Moss District Court, Norway and Amanda Hubbard, Trial Attorney, Computer Crime and Intellectual Property Division US Department of Justice, United States.

[236] http://www.itu.int/osg/spu/cybersecurity/agenda.html#session7

[237] http://www.itu.int/osg/spu/cybersecurity/agenda.html#session9

[238] http://www.itu.int/osg/spu/cybersecurity/agenda.html#session12

[239] http://www.itu.int/osg/spu/cybersecurity/agenda.html#session13

[240] http://www.itu.int/osg/spu/cybersecurity/agenda.html#session15

[241] http://www.itu.int/osg/spu/cybersecurity/agenda.html#session16

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