International Telecommunication Union

Australian Government
Department of Broadband, Communications and the Digital Economy

ITU Regional Cybersecurity Forum 2008 Brisbane, Australia

Document RFB/2008/01-E Rev.1
21 July 2008
Original: English

Meeting Report :

ITU Regional Cybersecurity Forum for Asia-Pacific and Seminar on the Economics of Cybersecurity, Brisbane, Australia, 15-18 July 2008[1]

Please send any comments you may have on this meeting report to cybmail(at)itu.int

Purpose of this Report

1. The ITU Regional Cybersecurity Forum for Asia-Pacific, and related Seminar on the Economics of Cybersecurity was held in Brisbane, Australia, 15-18 July 2008. The regional cybersecurity forum, which was hosted by the Department of Broadband, Communications and the Digital Economy (DBCDE), Government of Australia, aimed to identify the main challenges faced by countries in the region in developing frameworks for cybersecurity and CIIP, to consider best practices, share information on development activities being undertaken by ITU as well as other entities, and review the role of various actors in promoting a culture of cybersecurity.

2. The forum, one in a series of regional cybersecurity events organized by the ITU Development Sector (ITU-D), was held in response to ITU Plenipotentiary Resolution 130: Strengthening the role of ITU in building confidence and security in the use of information and communication technologies (Antalya, 2006) and the 2006 World Telecommunication Development Conference Doha Action Plan establishing ITU-D Study Group Question 22/1: *Securing information and communication networks: Best practices for developing a culture of cybersecurity*. As part of this activity, ITU is developing a *Report on Best Practices for a National Approach to Cybersecurity* which outlines a *Framework for Organizing a National Approach to Cybersecurity* identifying five key elements of a national cybersecurity effort, including: 1) Developing a cybersecurity strategy; 2) Establishing government – industry collaboration; 3) Creating incident management capability; 4) Deterring cybercrime; and 5) Promoting a culture of cybersecurity. The forum also considered initiatives on the regional and international level to increase cooperation and coordination amongst the different stakeholders.

3. Approximately 90 people from 27 countries participated in the event, from the Asia-Pacific region, the Pacific Islands, as well as from other parts of the world. Full documentation of the forum, including the final agenda and all presentations made, is available on the event website at www.itu.int/itu-d/cyb/events/2008/brisbane/. This meeting report[2] summarizes the discussions throughout the three days of the ITU Regional Cybersecurity Forum for Asia-Pacific, provides a high-level overview of the sessions and speaker presentations, and presents some of the common understandings and positions reached at the event. The day prior to the start of the ITU Regional Cybersecurity Forum for Asia-Pacific, 15 July 2008, was dedicated to an ITU Tariff Group for Asia and Oceania (TAS) Seminar on the Economics of Cybersecurity. Annex 1 at the end of this document includes a brief report from the Seminar on the Economics of Cybersecurity[3].

4. The one day Seminar on the Economics of Cybersecurity, was chaired by the Chairperson of ITU's Tariff Group for Asia and Oceania (TAS), Sahib Dayal Saxena from India. Throughout the seminar we learned about the pervasive incentives and the new revenue streams that are created from malware and spam, how they enable legitimate business models (e.g., anti-virus and anti-spam products, infrastructure, and bandwidth) as well as fraudulent and criminal ones (e.g., renting out of botnets, bullet proof hosting, commissions on spam-induced

---

[1] ITU Regional Cybersecurity Forum website: http://www.itu.int/ITU-D/cyb/events/2008/brisbane/

[2] This Forum Report is available online: http://www.itu.int/ITU-D/cyb/events/2008/brisbane/docs/brisbane-cybersecurity-forum-report-july-08.pdf

[3] The Report from the Seminar on the Economics of Cybersecurity can also be found online: http://www.itu.int/ITU-D/cyb/events/2008/brisbane/docs/brisbane-report-seminar-on-the-economics-of-cybersecurity-15-july-08.pdf

sales, pump and dump stock schemes). Distinguished experts in this area explained how malware and spam create mixed and sometimes conflicting incentives for stakeholders, which complicate coherent responses to the problem.

ITU Regional Cybersecurity Forum for Asia-Pacific held in Brisbane, Australia, 15-18 July 2008

5. As background information, considering that modern societies have a growing dependency on information and communication technologies (ICTs) that are globally interconnected, countries are increasingly aware that this creates interdependencies and risks that need to be managed at national, regional and international levels. Therefore, enhancing cybersecurity and protecting critical information infrastructures are essential to each nation's security, social and economic well-being. At the national level, this is a shared responsibility requiring coordinated action related to the prevention, preparation, response, and recovery from incidents on the part of government authorities, the private sector and citizens. At the regional and international level, this necessitates cooperation and coordination with relevant partners. The formulation and implementation of a national framework for cybersecurity and critical information infrastructure protection therefore requires a comprehensive, multi-disciplinary and multi-stakeholder approach. This Regional Cybersecurity Forum discussed some of the key elements in developing such policy and regulatory frameworks and proposed some concrete actions that can be taken in implementing these.

Meeting Opening and Welcome

6. The Regional Cybersecurity Forum for Asia-Pacific was opened with a welcoming address[4] by Keith Besgrove, First Assistant Secretary, Telecommunications, Network Regulation and Australia Post, Department of Broadband, Communications and the Digital Economy (DBCDE), Australia.

7. On behalf of DBCDE, Mr. Besgrove welcomed the forum participants to the event and highlighted why this regional cybersecurity event is an important step towards building cybersecurity capacity in the region. As the internet's impact on economies and society continue to increase, he noted, there is an overwhelming need to ensure confidence and security in the use of ICTs and the internet. As the internet has become a fundamental economic and social infrastructure, the misuse of ICTs for criminal purposes is also increasing. Cyber-attacks are becoming more sophisticated as cybercriminals become more organized, extending their operations beyond national borders. It is therefore vital that policy makers and regulators strive to become better connected and more organized than the criminals we are fighting, Mr. Besgrove continued. Therefore the need to engage in developing better, more broad-based, governance arrangements and policies is becoming a matter of increasing urgency and importance. This forum, Mr. Besgrove noted, has an important role to contribute in this context, and he thanked ITU for providing this opportunity to further discuss these issues.

8. Mr. Besgrove highlighted that internationally as well as domestically Australia has recognized the need to focus attention on e-security issues and believes in the need for an international approach to cybersecurity due to its borderless nature. Australia works collaboratively with international counterparts to effectively address these issues and actively participates in a range of international fora. Given the borderless nature of e-security threats, this kind of international engagement to focus attention, build networks and share information and experiences is extremely important in developing and consolidating appropriate responses to cybersecurity threats, he continued. From the point of view of a Member State (active in APEC, OECD, ITU, etc.), this is best done when organizations work within their areas of core competence, maintain a high degree of cooperation and information sharing both within their organizations, as well as with other organizations, in order to ensure efficiency and minimize the potential for duplication which would result in diluting the efforts that are being made. Mr. Besgrove concluded his opening remarks by highlighting that this Regional Cybersecurity Forum provides an opportunity for organizations and countries in the Asia-Pacific region to come together to share experiences, and work towards their common objective in promoting a culture of cybersecurity that will foster an inclusive, secure and global information society.

9. Eun-Ju Kim, Head, ITU Regional Office for Asia and Pacific[5] followed with some opening remarks[6] on behalf of the ITU and the Director of the ITU Telecommunication Development Sector (ITU-D), Sami Al Basheer Al Morshid. Ms. Kim said that she was thrilled to see so many distinguished speakers from the region as well as experts who have traveled from afar to gather for this meeting. She noted that as the list of speakers and participants was very impressive she was sure this event would be beneficial to everyone and contribute to a deeper understanding of this very interesting subject. Ms. Kim brought the participants' attention to the fact that cyber-threats have become increasingly sophisticated since the early 1980s, when the first known case of a computer virus was reported. Today, cybercrime has created an organized underground economy reaping vast financial rewards using sophisticated software tools that threaten users and information infrastructures in all countries. Sometimes the biggest threats are simple accidents. This was demonstrated only a few months ago when millions of users in the Middle East were impacted by cuts in undersea optical cables — said to be caused

[4] http://www.itu.int/ITU-D/cyb/events/2008/brisbane/docs/dbcde-opening-remarks-brisbane-july-08.pdf

[5] http://www.itu.int/ITU-D/asp/

[6] http://www.itu.int/ITU-D/cyb/events/2008/brisbane/docs/itu-opening-remarks-brisbane-july-08.pdf

by a boat anchor. In fact, Ms. Kim continued, it also happened here in the Queensland, Australia, yesterday morning, when she was trying to submit some documents online. As a result, in these cases, access to the internet, voice calls, corporate data and video traffic were all impacted in one way or the other. In the Australian case, we learned that the Australia government and industry requested backup after the optical cable disruption. Just a few weeks ago, Ms. Kim explained, we also saw one of the countries in this region, more specifically the Marshall Islands, experience disruptions that paralyzed e-mail communications in the country. Reports say that hackers had launched a zombie computer attack on the western Pacific nation's only ISP. It has been said that experience is the hardest teacher, because it gives the test first and the lesson afterwards. Whatever the cause, whether intentional or not, cybercrime or a mundane accident, the lesson we take away from these incidents, Ms. Kim said, is that every nation needs to prepare and organize itself to take comprehensive and coordinated actions related to the prevention of, preparation for, response to, and recovery from cyber incidents.

10. As cybersecurity-related goals and tasks ahead of nations are huge in importance and resources are limited, Ms. Kim continued, ITU is committed to working together with the membership to come to a common understanding on the importance of promoting a global culture of cybersecurity. In the ITU's Development Sector, this is done through our programmes and initiatives that were developed at the WTDC in Qatar and approved at the Plenipotentiary Conference in Turkey in 2006. Ms. Kim further noted that ITU is aware that the issues raised by the ITU membership are real needs that require close cooperation from both the public and private sector to ensure that that all the citizens of the world can have improved access to ICTs — which hopefully will improve their lives and economical and social status.

11. Furthermore, she continued, recognizing the importance of international cooperation for cybersecurity, just over a year ago on 17 May 2007, ITU launched the Global Cybersecurity Agenda (GCA), which is the ITU framework for international cooperation. The GCA builds on existing national, regional and international initiatives to avoid duplication of work and encourage collaboration amongst all relevant partners. Ms. Kim shared with the forum participants some of the recent initiatives by ITU Secretary-General in this regard. This includes, collaboration with the International Multilateral Partnership Against Cyber Terrorism (IMPACT) initiated by the Malaysian Prime Minister, a series of meetings with the Japanese Prime Minister and numerous ministers during OECD Ministerial in Seoul with the objective of combating cybercrime as well as addressing climate change, and a special High Level Segment session on the cybersecurity at the forthcoming 2008 ITU Council. Ms. Kim called out to organizations and countries that may be interested in exploring possibilities for collaboration with the ITU to meet the GCA goals, to contact the Secretariat. Ms. Kim concluded her opening remarks by thanking the Government of Australia, especially the Department of Broadband, Communications and the Digital Economy (DBCDE), for the never-ending efforts and generous hospitality in organizing this event with the ITU, and wished the participants and organizers a successful event.

12. These opening remarks were followed by opening remarks[7] by Joong Yeon Hwang, President and CEO, Korea Information Security Agency (KISA), Republic of Korea. Mr. Hwang provided an insight into the activities of KISA, Korea's specialized organization for information security. He noted that the cybersecurity issue is a transnational one as all systems and networks are interconnected through the internet. Therefore, it is not enough if each country or stakeholder makes a full effort to strengthen the security of its own information systems and networks. As long as all countries and stakeholders do not contribute to making the internet secure and safe together, substantial damage can be done to each one's own key assets, critical information infrastructures, and further to other stakeholders connected to the internet. Mr. Hwang noted some key characteristics of recent emerging cybersecurity issues, including for instance, the emergence of botnets which can cause one victim to become the attacking vector for another victim. He also mentioned the adoption of Next Generation Networks and the transition to a Ubiquitous Network Society which makes the need to consider the security aspect of all connected devices one of the highest priorities. Without the security, Mr. Hwang continued, it is very challenging to gain all the possible positive impacts of ICT implementation and adoption.

13. Mr. Hwang concluded his remarks by emphasizing awareness raising on internet security for the general user as one of the most critical issues that we are currently faced with. He noted that cybersecurity calls for close cooperation among all the stakeholders, including government, business, academia and civil society. Although the leading role and efforts driven by government is critical in each economy, it is impossible to be successful without collaboration with the private sector, including with Internet Service Providers. This cooperation also needs to expand beyond domestic relationship boundaries to the regional and global cooperation arena. Therefore, in order to narrow the cybersecurity gap, all countries need to work together. KISA, he continued, can be seen as a reliable partner within the global cybersecurity framework and KISA hopes to initiate practical and continuous collaborative partnerships with ITU to assist developing countries and relevant stakeholders in this regard. Mr. Hwang thanked ITU and the Australian Government for giving KISA the opportunity to be a part of this informative regional cybersecurity forum.

[7] http://www.itu.int/ITU-D/cyb/events/2008/brisbane/docs/kisa-opening-remarks-brisbane-july-08.pdf

Session 1: Towards a Framework for Cybersecurity and Critical Information Infrastructure Protection

14. The necessity of building confidence and security in the use of ICTs, promoting cybersecurity and protecting critical infrastructures at national levels is generally acknowledged. As national public and private actors bring their own perspective to the relevant importance of issues, in order to have a consistent approach, some countries have established institutional frameworks while other countries have used a light-weight, non-institutional approach. Many countries have not yet established a national strategy for cybersecurity and CIIP. This first session, chaired by Keith Besgrove, First Assistant Secretary, Telecommunications, Network Regulation and Australia Post, Department of Broadband, Communications and the Digital Economy (DBCDE), Australia, introduced the concept of a national framework for cybersecurity and CIIP and presented some of the ongoing efforts to elaborate a best practices framework in the ITU, in order to provide meeting participants with a broad overview of the issues and challenges involved. Mr. Besgrove noted that the purpose of this event is to help countries better understand the dependencies and interdependencies that interconnection creates, and to assist countries in developing national frameworks for cybersecurity.

15. Christine Sund, Cybersecurity Coordinator, ICT Applications and Cybersecurity Division, ITU Telecommunication Development Sector (ITU-D), in her presentation provided an overview of "ITU-D Activities Related to Cybersecurity and Critical Information Infrastructure Protection"[8] and shared details on the ITU-D Cybersecurity Work Programme to Assist Developing Countries (2007-2009)[9], with specific examples of what the ITU is trying to do to help developing countries in the domain of cybersecurity and CIIP. Some of the ongoing and planned ITU cybersecurity initiatives mentioned in his presentation included: activities dealing with the identification of best practices in the establishment of national frameworks for cybersecurity and CIIP; a national cybersecurity/CIIP readiness self-assessment toolkit; a botnet mitigation toolkit; cybersecurity guideline publications for developing countries; an international survey of national cybersecurity/CSIRT capabilities; a toolkit for model cybercrime legislation for developing countries; a toolkit for promoting a culture of cybersecurity as well as a number of planned regional events for awareness-raising and capacity building on frameworks for cybersecurity and CIIP.

16. Ms. Sund further noted that most countries have not yet formulated or implemented a national strategy for cybersecurity and critical information infrastructure protection, and that with limited human, institutional and financial resources, developing countries face particular challenges in elaborating and implementing such policies. The ITU Telecommunication Development Sector has a Study Group Question, Study Group 1 Question 22, currently developing a best practices document containing a proposed framework for national cybersecurity efforts which is closely tied to the *ITU-D Cybersecurity Work Programme to Assist Developing Countries*. This *Work Programme* describes how ITU plans to assist countries in developing cybersecurity/CIIP capacity, through providing Member States with useful resources, reference material, and toolkits on related subjects. As the related toolkits become more stable, the ITU-D is looking to disseminate them widely through multiple channels to ITU's 191 Member States.

17. Ms. Sund continued with an overview of the work on a *Framework for National Cybersecurity Efforts* that is currently being developed in ITU-D Study Group 1 Question 22—*Securing Information and Communication Networks: Best Practices for Developing a Culture of Cybersecurity*. She explained the background of work in the Study Group and particularly its report on *Best Practices for Organizing National Cybersecurity Efforts*[10], which governments can use as a guideline when developing and undertaking national strategies for cybersecurity and CIIP. Four Study Group Q22/1 meetings have taken place to date, with the next meeting scheduled for 8-9 September 2008. The report being developed by the Study Group addresses the major problems that policy makers are faced with when dealing with cybersecurity. The *Framework for National Cybersecurity Efforts* elaborated on in the report, looks at five main components for best practices in cybersecurity, namely: 1) A National Strategy for Cybersecurity; 2) Government – Industry Collaboration; 3) Deterring Cybercrime; 4) Incident Management Capabilities; and, 5) A Culture of Cybersecurity. Ms. Sund invited forum participants and country representatives to join the Q22/1 activities.

18. Joseph Richardson, Consultant, United States of America, continued by providing a more detailed insight into the "Management Framework for Organizing National Cybersecurity/CIIP Efforts" and the "ITU National Cybersecurity/CIIP Self-Assessment Toolkit"[11]. Mr. Richardson went into further detail on the Management Framework for Organizing National Cybersecurity/CIIP Efforts, which forms the structure behind the draft report from ITU-D Study Group 1 Question 22. The Framework includes a policy statement for each component of the framework, identifies goals and specific steps to reach these goals, and references and material related to each

[8] http://www.itu.int/ITU-D/cyb/events/2008/brisbane/docs/sund-itu-d-cybersecurity-overview-brisbane-july-08.pdf

[9] http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-cybersecurity-work-programme-developing-countries.pdf

[10] http://www.itu.int/md/D06-SG01-C-0130/en *(ITU TIES login and password required)*. A draft document providing more information on the ITU Framework for Cybersecurity can also be found at http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-draft-cybersecurity-framework.pdf

[11] http://www.itu.int/ITU-D/cyb/events/2008/brisbane/docs/richardson-cybersecurity-overview-and-self-assessment-toolkit-brisbane-july-08.pdf

specific step. Mr. Richardson further noted that the *Best Practices for Organizing National Cybersecurity Efforts* report, including the framework, is a living document and as such, will evolve over time. Highlighting that the protection of cyberspace is essential to national security and economic well-being, Mr. Richardson continued by provided some concrete ideas on how countries can get started on developing a national cybersecurity strategy. An important tool in this effort is the ongoing ITU work to develop a comprehensive National Cybersecurity/CIIP Self-Assessment Toolkit[12]. As one of the linkages between the ITU-D Study Group Q22/1 work on "Securing information and communication networks: Best practices for developing a culture of cybersecurity"[13] and the ITU Cybersecurity Work Programme to Assist Developing Countries (2007-2009)[14] activities, the ITU National Cybersecurity/CIIP Self-Assessment Toolkit shows how the framework under development in the Study Group with a practical toolkit for consideration at the national level.

19. The toolkit can assist governments in examining existing national policies, procedures, norms, institutions and other elements necessary for formulating security strategies in an ever-changing ICT environment. It can help governments better understand existing systems, identify gaps that require special attention and prioritize national response efforts. The toolkit addresses the management and policy level for each of the five elements of the best practices framework presented earlier. Mr. Richardson highlighted that the toolkit identifies issues and poses a number of questions that might be worth considering; what actions have been taken to date, what actions are planned, what actions are to be considered, what is the status of these actions? Mr. Richardson also noted that no country is starting at zero when it comes to initiatives for cybersecurity. Furthermore, there is no one right answer or approach as all countries have unique national requirements and desires. Continual review and revision is needed of any approach taken, and it is equally important to involve all stakeholders, appropriate to their roles, in developing a national strategy. Countries interested in undertaking a facilitated national cybersecurity/CIIP self-assessment together with the ITU is welcome to contact the ITU Development Bureau at cybmail@itu.int[15].

20. Mike Rothery, Assistant Secretary of Critical Infrastructure Protection, Attorney-General's Department, provided an insight into some of the main "Critical Infrastructure Protection Issues in Australia"[16] and how these are being addressed. Mr. Rothery noted that Australia is currently in the middle of a review of their strategy for cybersecurity and critical infrastructure protection. The reason for this review is that the size and scale of the threat is changing and dependencies involved are growing rapidly. Every part of the government is contributing to making the problem bigger, he continued, as the government agencies are putting more information, including citizens' personal information, on computers and devices, and on the internet. With this the problem is moving from marginal to the mainstream. One of the main challenges in addressing issues in the changing cyber-threat environment, he continued, is recruiting people who have a good overall understand of ICTs and security. He also noted that stolen data, for instance, is on sale, and the world has already experienced many instances where tax payers records have been lost, bank account details have gone missing, but no rule or law was broken in the process because the rule said that the tax payers' records are to be treated as paper. With this example Mr. Rothery pointed out that rules and legislation have not kept up to speed with the changes that have taken place in this area.

21. The Australian policy for cybersecurity, he continued, is based on three main pillars: 1) Reducing the e-security risk to Australian Government information and communications systems; 2) Reducing the e-security risk to Australia's national critical infrastructure; and 3) Enhancing the protection of home users and SMEs from electronic attacks and fraud. However, Australia has realized that the main parties and players are not directly part of any of these three pillars. Due to this, for example, security decisions are not being made by the IT industry where the focus is on accessibility, speed, and moving more work to the internet. A lot of things can be done, Mr. Rothery continued, from awareness raising to regulation. In Australia there is willingness to regulate for government users and uses but reluctance to regulate for private users. One reason for this is the fact that we cannot keep up to speed on what is happening in the larger internet user community and if everything is regulated there is a risk that the government stifles growth and related opportunities. Mr. Rothery also noted that he was not entirely sure that a solution that fits one industry necessarily fits the others too, and therefore the Australian government is not recommending additional regulation at this time. The question can also be whether regulation should or should not be centralized in one area? Australia has a more decentralized approach but this is not quite working either. Because all the different factors involved, any approach taken in this regard needs to be balanced one, he continued.

22. Mr. Rothery continued sharing some insights into what Australia is doing to address the challenges involved. He noted that while there are parts of government that are specifically responsible for the uptake of ICTs, like

---

[12] http://www.itu.int/ITU-D/cyb/cybersecurity/projects/readiness.html

[13] http://www.itu.int/ITU-D/cyb/cybersecurity/index.html

[14] http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-cybersecurity-work-programme-developing-countries.pdf

[15] Countries interested in undertaking a facilitated national cybersecurity/CIIP self-assessment together with the ITU as welcome to contact the ITU Development Bureau at cybmail@itu.int.

[16] No slides available.

the DBCDE, all departments need to be on top of what is happening in this area as they all have a specific role to play. He said that there is a clear need for leadership and policy setting in this area, but at the same time, other parts of the government cannot be let off the hook. In this regard, Australia is now heading for some kind of hybrid solution. There are people in the central government who play a leadership role but at the same time there is an overall need to make cybersecurity a mainstream problem and not a centralized problem where only one part of government is directly involved. Everyone should be aware of how they need to consider and integrate cybersecurity into their specific area of responsibility. The right environment needs to be put in place to make them feel responsible and integrate it into their decision making processes. With the review of the current policy, Australia has realized that on the national level, they need to integrate cybersecurity better.

23. Before breaking for lunch, the Forum participants had the honor of listening to a ministerial address[17] by Senator Stephen Conroy, Minister for Broadband, Communications and the Digital Economy (DBCDE), Australia on the issue of cybersecurity. In his address to the Regional Cybersecurity Forum, Senator Conroy stressed the importance of the meeting for the economies of all nations represented, and noted that this meeting is a very important discussion between neighbors. By giving an example of a recent security incident he drew the forum participants' attention to the fact that even peak bodies—even those that should have the most awareness of e-security measures—are vulnerable to attack if their security policies are not maintained. Therefore, he noted, none of us can afford to relax. He continued by mentioning that the Australian Government is committed to working with other nations to create safer online environments. We see the developing digital economy as offering great benefit to all nations of the world, he said. The internet is a powerful tool for seeking and storing information and entertainment, but this can work against our interests as much as for them. We need to set up safeguards against the criminal exploitation of the online world. We need the software and security protocols to safeguard our financial transactions. We need firewalls to protect our homes and workplaces against intrusions that invade our privacy and steal personal information and identities. We need filters and other tools that will ensure our children and families are not exposed to danger or distress during their online activities. And we need the skilled law enforcement agencies to track undesirable online activities.

24. True online security and success in the digital economy, he continued, require the foundations of international agreement on security standards and protocols and a commitment to effectively enforce them. The purpose in having these common standards and protocols, Senator Conroy stressed, is to build trust and confidence in our online transactions—in banking, negotiation and trade in the electronic marketplace. Without trust, we are forever suspicious—looking over our shoulder. He further noted that the low levels of consumer confidence in the security and privacy of transactions on the internet remain significant barriers to achieving the potential of the internet economy. As the e-security landscape is constantly changing with the emergence of new and more sophisticated online threats, in his address Senator Conroy shared insights into some of the targeted initiatives that the Australian Government is delivering in responding to these real threats. He also noted that OECD's work on e-security will assist the ITU to access international best practices and this in turn will help ITU to contribute to global efforts. The ITU is uniquely placed to support developing countries that are in the initial phases of formulating cybersecurity strategies, he said.

25. When stressing that collaboration between government, industry and users is crucial when developing strategies to deal with e-security threats that undermine confidence and trust in the online environment, Senator Conroy announced an initiative, a scoping study into the creation of a Computer Emergency Response Team in the Pacific. Computer Emergency Response Teams (CERTs) are a crucial aspect of a broader e-security strategy. CERTs can provide a coordinated approach to informing key stakeholders of the latest cyber-threats and assist in developing coordinated responses to these threats. Senator Conroy noted that the Department and the Attorney-General's Department have held, over the past 12 months, a series of informal discussions with key stakeholders in the Pacific ICT community as the Departments have been keen to learn how best to support them to set up a Pacific-based CERT. The initial study, as a ways to determine the best path forward for establishing a Pacific-based CERT, is a result of Australia's contributions to the ITU and collaboration with AusCERT.

26. When all countries, including countries in the Pacific region, are able to access computer incident prevention, response and mitigation strategies, they can respond in a timely manner to threats affecting or involving their telecommunications networks. Senator Conroy emphasized that the success of a CERT for the Pacific region will depend greatly upon agreed protocols and standards and a commitment by all participating nations to maintain and enforce them. In conclusion, he noted that success in the digital economy requires more cooperation—not less. The benefits of the digital economy will flow only to those nations that embrace its potential for establishing access and commonality in purpose. This does not mean relinquishing national identity or sovereignty. Rather, it requires engagement in the global marketplace on terms that inspire trust and confidence and in international fora such as this. Senator Conroy noted that the regional cybersecurity forum is a firm step down that path.

[17] http://www.itu.int/ITU-D/cyb/events/2008/brisbane/docs/conroy-ministerial-address-brisbane-july-08.pdf

Session 2: Management Framework for Organizing National Cybersecurity/CIIP Efforts and Country Case Studies: Promoting a Culture of Cybersecurity

27. In order to better understand the Management Framework for Organizing National Cybersecurity/CIIP Efforts and further explore how different countries are currently implementing the five pillars of the Framework, i.e. Promoting a Culture of Cybersecurity, Government – Industry Collaboration, Legal Foundation and Enforcement, Incident Management Capabilities, and Developing a National Cybersecurity Strategy, sessions 2, 3, 4, 5, and 6 were dedicated to the specific pillars and related country case studies. Session 2, moderated by Richard Beach, Senior NetSafe Consultant, NetSafe – The Internet Safety Group, New Zealand, looked closer at the building blocks needed to successfully Promote a Culture of Cybersecurity.

28. Christine Sund, Cybersecurity Coordinator, ICT Applications and Cybersecurity Division, ITU Telecommunication Development Sector (ITU-D), in her presentation on "Promoting a Culture of Cybersecurity – Fundamentals"[18] provided an overview of what a culture of cybersecurity means and some of the possible roles of different stakeholders in the Information Society in creating a global culture of cybersecurity. She highlighted nine elements for creating a culture of cybersecurity as stated in UN Resolution 57/239 (2002): "Creation of a global culture of cybersecurity", and UN Resolution 58/199 (2004): "Promotion of a global culture of cybersecurity and protection of critical information infrastructures". These nine elements included: a) awareness, b) responsibility, c) response, d) ethics, e) democracy, f) risk assessment, g) security design and implementation, h) security management, and i) reassessment. Through these Resolutions, UN Member States and all relevant international organizations were asked to address and take these elements into account in preparation for the two phases on the World Summit on the Information Society (WSIS)[19] in 2003 and 2005. The outcome documents from the two WSIS phases further emphasized the importance of building confidence and security in the use of ICTs and countries' commitment to promoting a culture of security.

29. Ms. Sund's presentation mentioned some possible roles for governments in promoting a culture of cybersecurity, including: ensuring that a nation's citizens are protected; playing a central role in coordinating and implementing a national cybersecurity strategy; ensuring that the national policy is flexible and adaptive; coordinating responsibilities across authorities and government departments; creating new (or adapting existing) legislation to criminalize the misuse of ICTs; to curb abuses and to protect consumer rights; and to lead national, regional, and international cybersecurity cooperation activities. Ms. Sund emphasized that as ICT infrastructures are in many countries for the most part owned and operated by the private sector, their involvement in promoting a national and global culture of cybersecurity is crucial. Effective cybersecurity needs an in-depth understanding of all aspects of ICT networks, and therefore the private sector's expertise and involvement are paramount in the development and implementation of national cybersecurity strategies. Furthermore, Ms. Sund highlighted that governments and businesses need to assist citizens to obtain information on how to protect themselves online. With the right tools readily accessible, each participant in the Information Society is responsible for being alert and protecting themselves while noting that cybersecurity at its core is a shared responsibility.

30. Kathryn Kerr, Manager, Analysis and Assessments, AusCERT, Australia, with her overview of the findings from a recent "AusCERT Home Users Computer Security Survey"[20], highlighted the need to find a balance between users' confidence and their understanding that there is a risk involved when doing things online. The AusCERT Home Computer Users Security Survey 2008[21] was prepared to assess the security posture of Australian-based home internet users, their level of security awareness and attitudes to internet security. The final survey report, Ms. Kerr said, was written primarily for home internet users to help raise their awareness of internet computer security issues. The survey was conducted in March 2008 and resulted in 1001 answers. The survey sought to examine a random sample of Australia-based home computer users with internet connections who conduct activities online, looking at what these users are doing with the security awareness training that they receive and investigating whether there is a correlation between riskier behavior and configurations online and incidents of malware infections. Recognizing that a range of factors affect whether users' computers get compromised and that the survey instrument might not able to capture all relevant aspects of this, including some users' lack of awareness of their own configurations, etc.

31. Interestingly the survey showed that 38 per cent of those who answered the survey believe they can rely on anti-virus or anti-spyware software to alert them to malware infections. Yet, at the same time, Ms. Kerr noted, approximately 40 per cent of malware are not detected, across vendors. Another interesting result was that one third of those who do not use anti-phishing tools (making up 57 per cent of respondents) do not know what a phishing site is, yet phishing is a common form of attack that targets computer users and has been in the Australia media since 2003. The findings of the survey further highlighted the need for people to understand the

---

[18] http://www.itu.int/ITU-D/cyb/events/2008/brisbane/docs/sund-promoting-a-culture-of-cybersecurity-brisbane-july-08.pdf

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

[20] http://www.itu.int/ITU-D/cyb/events/2008/brisbane/docs/kerr-auscert-user-survey-brisbane-july-08.pdf

[21] The full 2008 survey is available online at: http://www.auscert.org.au/usersurvey

limitations of technology when they take their computers and devices online. Overall the survey showed that risky online practices were common among home internet users.

32. Philip Victor, Head, Training and Outreach, CyberSecurity Malaysia, Malaysia followed with a country case study, "Promoting a Culture of Cybersecurity — Malaysia Case Study"[22]. He started by introducing CyberSecurity Malaysia, which had started as the Malaysian Computer Emergency Response Team (MyCERT) already in 1997. In 2001 the team assumed a larger role in protecting Malaysia's Cyber Space as NISER, the National ICT Security & Emergency Response Centre, and in 2005 it was a company under the Ministry of Science, Technology, and Innovation, and in 2006 it assumed the role of national cyber security agency. The Malaysian National Cyber Security Policy was initiated by the Ministry of Science, Technology and Innovation in 2006 to harness national efforts to facilitate Malaysia's move towards a knowledge-based economy and enhance the security of Malaysia's Critical National Information Infrastructure (CNII). The policy is structured around eight main cybersecurity policy thrusts, similar to the five pillars of the ITU National Cybersecurity Framework but where some of these pillars have been broken up further to meet specific Malaysian requirements. Each policy trust is lead by a lead ministry/agency. One of the policy thrusts is dedicated to a "Culture of Security & Capacity Building", and includes developing, fostering and maintaining a national culture of security as well as standardizing and coordinating cybersecurity awareness and education programmes across all elements of the Malaysian CNII. The Ministry of Science, Technology, and Innovation, leads the Culture of Security & Capacity Building trust.

33. Establishing an effective mechanism for cybersecurity knowledge dissemination at the national level and identifying minimum requirements and qualifications for information security professionals are also important parts of the information security competency development activity. When it comes to the education of endusers Mr. Victor shared an insight into the outreach programs that are being undertaken by CyberSecurity Malaysia. In promoting a safer and more secure online environment CyberSecurity Malaysia is trying to make people understand that the internet is useful for many things and holds a magnitude of useful resources, but while online people have to take care. CyberSecurity Malaysia's outreach programs aim to build a culture of security through specific awareness programs to the different target groups; be they kids and teenagers, parents and professionals or companies and organizations. Short videos, television commercials, newsletters, posters, publications, workshops and conferences provided in Bahasa Malaysian and English, are some of the specific activities that have been delivered in the past. The need to be innovative and generate material specific to the target audiences and to expand partnerships with key stakeholders in order to better reach out to the end users was highlighted throughout Mr. Victor's presentation.

34. Mr. Victor concluded his presentation with some lessons learned over the past few years and some ideas for how countries and organizations can contribute towards making cyberspace more secure. He noted here that information security strategies must cover all different kinds of user groups, with targeted and customized approaches. Awareness and education for enhanced cybersecurity must be deployed throughout the entities and organizations, and include all vendors, alliance and related stakeholders. Public-private cooperation is furthermore critical to building a culture of security, he continued, mentioning also that the adoption of international standards and best practices for security creates a competitive advance at the level of nation states as well as for individual companies. Finally, security is everyone's responsibility and needs to start at the top, with endorsement and understanding at the highest possible level.

35. Richard Beach, Senior NetSafe Consultant, NetSafe[23] — The Internet Safety Group, New Zealand, continued with his presentation on "Promoting a Culture of Cybersecurity — New Zealand Case Study"[24] showing how cybersecurity awareness raising and training, and other NetSafe activities, fit in as an 'enabler' under the 'Confidence' strand of New Zealand's Digital Strategy. The overall Digital Strategy is built around three different areas, i.e. Government, Business and Communities, and three supporting strands that impact on all of these, namely Connection, Content, and Confidence. Mr. Beach shared with the forum participants some of the ongoing initiatives that NetSafe is involved in three different areas. First, when it comes to encouraging a culture of security in business enterprises, with the many small businesses active in the country, New Zealand and NetSafe have for instance special initiatives to address cybersecurity for small and medium sized enterprises (SMEs). The SME Toolkit is based on a self-assessment process which can help companies develop a policy framework and training plan framework, and also consists of community spaces as well as self-paced training courses. Second, with special attention to the needs of children and individuals, two main cybersafety programmes have been developed. One is the Netsafe Kit for Schools and the other is the NetSafe Kit for ECE. In this context Mr. Beach also discussed a possible "Cybercitizenship Pathway" which aims to assist cybercitizens mange their use of ICT with integrity and confidence. The Pathway aligns with national school curriculum and integrates cybercitizenship across curriculum areas. Mr. Beach also shared information on well-known awareness raising NetSafe campaigns and approaches for which the impact has reached well beyond New Zealand's national borders including Hector's World™, The NetBasics, etc. Third, with regards to a national awareness program, all stakeholder can learn more through the www.netsafe.org.nz web portal where targeted material and training

[22] http://www.itu.int/ITU-D/cyb/events/2008/brisbane/docs/victor-malaysia-culture-of-cybersecurity-brisbane-july-08.pdf

[23] http://www.netsafe.org.nz

[24] http://www.itu.int/ITU-D/cyb/events/2008/brisbane/docs/beach-nz-casestudy-culture-of-security-brisbane-july-08.pdf

resources are shared to help the different kinds of users learn how to ensure the internet safely. In conclusion Mr. Beach provided an insight into what he sees as key challenges when promoting a culture of cybersecurity, mentioning here the 1) low media interest in positive initiatives, 2) human response to 'non-immediate' threats, 3) lack of funding, 4) no clear path, as this is cutting edge, and 5) the difficulty of measure success.

36. At the end of the sessions, with the help of a practical exercise, Joseph Richardson, helped the forum participants better understand how they can use the ITU National Cybersecurity/CIIP Self-Assessment Toolkit[25] to assess national cybersecurity readiness for each of the different topics. The self-assessment process overall is intended to help governments understand their existing efforts, identify gaps that require attention, and prioritize national efforts and practical implications of the initiatives that they are putting in place. In conducting the facilitated self-assessment, guiding the countries through the self-assessment process, Mr. Richardson noted that there is no one right answer or approach as all countries have unique national requirements and desires. A continual review and revision is needed of any approach taken and it is equally important to involve all stakeholders, appropriate to their roles, in developing all the components needed for an overall national strategy for cybersecurity and CIIP. Mr. Richardson mentioned that updates to the toolkit and related resources are continuously made through the ITU-D cybersecurity website (www.itu.int/ITU-D/cyb/cybersecurity/projects/readiness.html), and country pilot projects to test and evaluate the toolkit are being undertaken in conjunction with a number of regional capacity-building events and workshops organized by ITU in 2008, and 2009.

Session 3: Management Framework for Organizing National Cybersecurity/CIIP Efforts and Country Case Studies: Government — Industry Collaboration

37. The next session looked closer at the Government — Industry Collaboration pillar of the Management Framework for Organizing National Cybersecurity/CIIP Efforts and Country Case Studies. This session was moderated by Tua'imalo Asamu Ah Sam, Chief Executive Officer, Ministry of Communications and Information Technology, Independent State of Samoa.

38. Steve Stroud, Director, Attorney-General's Department, Australia, started his presentation on "Government-Industry Collaboration: An Australian Case Study"[26] by highlighting some of the specific roles of the government in cybersecurity and critical information infrastructure protection. Here he mentioned the role of the government to work with owners and operators of critical infrastructures to: facilitate cooperation and information sharing; identify risks and develop suitable responses to these risks; and clearly set out and establish roles and responsibilities. Mr. Stroud also shared some lessons learned from Australia's recent national cybersecurity exercise, the Cyber Storm II, which incorporated various levels of government and private sector players. It was the largest government sponsored cyber exercise of its kind in Australia. In total 56 Australian organizations took part in Cyber Storm II according to Mr. Stroud who headed Australia's Cyber Storm II effort. The Government provided a framework, which allowed participating organizations the opportunity to conduct do an internal exercise at the same time alongside their suppliers and customers. This allowed external communications channels that would normally be notional to be practiced.

39. In total 200 people participated in planning the Australian exercise, including both old and new "players". Mr. Stroud noted that introducing new players into the exercise is fine and adds value as experienced player educate and train the new players. The exercise execution Included a law enforcement and intelligence build up during between two to four weeks, three days of actual play, and one day of "hot wash". A common finding was that delegates in the incident response teams of participating organizations sometimes became short-sighted under the simulated attacks, leading to chains of command crumbling, careless mistakes, and the loss of vital information. Many organizations wanted to exercise senior incident response boards, and to do that they had to create a crisis on the shop floor. What they found out was that it was very hard to get people to escalate problems to senior management. The incident response teams were putting out spot fires here and there and no one took a step back to see that the whole house was on fire.

40. Julie Inman Grant, Regional Director, Internet Safety and Security, Microsoft Asia Pacific, in her presentation on "Critical Infrastructure Protection: Collaboration, Policy Drivers and the CIP Continuum"[27] provided an overview of the trust component key to building and maintaining partnerships at all levels. She noted that building and maintaining trustworthy partnerships, policies, and practices requires a clear value proposition, defined roles and responsibilities, and above all trust. These partnerships are not easy to establish, but they are an essential foundation for the trusted collaboration needed to realize critical infrastructure security goals. In her presentation, Ms. Inman Grant defined Microsoft's perspective on CIP and the key elements of collaboration and partnership, including role definition. She outlined Microsoft's vision for what she called, a "CIP Continuum", with a particular focus of the critical policy drivers for success in Asia Pacific. In addition, Ms. Inman Grant shared some of the main results of a recent (cybercrime, privacy, spam and child protection) legislative survey

---

[25] http://www.itu.int/ITU-D/cyb/cybersecurity/projects/readiness.html

[26] http://www.itu.int/ITU-D/cyb/events/2008/brisbane/docs/stroud-australia-gov-industry-collaboration-brisbane-july-08.pdf

[27] http://www.itu.int/ITU-D/cyb/events/2008/brisbane/docs/inman-cip-continuum-collaboration-brisbane-july-08.pdf

that has been conducted by Microsoft in the region. The initial iteration of this study was conducted in 2005, and in October 2007, Microsoft finished updating the study to reflect recent developments in the region and made this study public.

41. The analysis covers the fourteen jurisdictions. Ms. Inman Grant noted that one of Microsoft's objectives in undertaking the study was to gain an understanding of how the laws of different jurisdictions compared against one single benchmark. To this end, they selected benchmark instruments for each of the four areas of law and analysed the domestic laws of the fourteen jurisdictions above against these. Noting that of the four areas analysed, computer security was the most developed with 13 of the 14 countries having computer security laws in place. Comparatively, less legislative activity in the Asia Pacific region was seen in the privacy and data protection space. Laws which specifically address privacy and data protection issues had only been enacted in six of the fourteen jurisdictions studied. Of the countries that have privacy laws in place, their regimes are quite varied. This divergence is not surprising considering that there is no global data protection norm against which legislative proposals can be assessed. Interestingly, in the area of spam half of the fourteen countries studied have comprehensive spam legislation in place. Three other jurisdictions have laws that broadly, though not comprehensively, address the sending of unsolicited electronic messages. On the other hand, online child safety laws were the least well developed vis-à-vis the benchmark legislation, although to some extent this can be explained by varying cultural forces and approaches to content regulation in the region.

42. The evening of the first full day of the forum the participants were invited by the organizers to a reception at the event venue.

Session 4: Management Framework for Organizing National Cybersecurity/CIIP Efforts and Country Case Studies: Legal Foundation and Enforcement

43. Appropriate legislation, international legal coordination and enforcement are all important elements in preventing, detecting and responding to cybercrime and the misuse of ICTs. This requires updating of criminal law, procedures and policies to address cybersecurity incidents and respond to cybercrime. As a result, many countries have made amendments in their penal codes, or are in the process of adopting amendments, in accordance with international conventions and recommendations. Session 4 looked closer at the need for a sound legal foundation and effective enforcement. The Session 4 moderator, Adrian McCullagh, Professor, Telecommunications & Secure E-Business Law, Information Security Institute, Queensland University of Technology, Australia introduced the speakers in the session, and highlighted the growing problems related to different legal frameworks in countries around the world and the need for increased collaboration between all countries in this regard.

44. Marco Gercke, Lecturer, University of Cologne, Germany, provided the first presentation in the session with an insight into some of the "Legal Foundation and Enforcement Fundamentals"[28], highlighting what is currently happening in the international community with regards to countries' revising existing laws and developing new legislation to criminalize the misuse of ICTs. Mr. Gercke noted that there are constantly new offenses and new challenges when it comes to the internet. Therefore, national legislation constantly needs to be revised and updated. Countries and stakeholders involved first need to look at the technology, see how it is being misused, and then protect the users through new legislation, keeping in mind that there is always a time gap between recognizing a crime and law adjustments. While there are many internet-related challenges that need to be addressed with legal solutions, he continued, not all challenges need legal solutions. Therefore countries should not start thinking about criminalizing things on the internet that would not be criminalized outside of the internet. A legal foundation provides the framework to investigate, prosecute and deter cybercrime, promote cybersecurity, as well as provide confidence in legal systems and encourage commerce.

45. While elaborating on some of the existing national, regional and international cybercrime legislation, Mr. Gercke emphasized the need for and importance of further harmonisation of legislation and referred to the Budapest Convention on Cybercrime[29] (2001) as one of the main international frameworks currently available. He noted that there are a number of international initiatives for cybersecurity and the fight against cybercrime, and that all these different initiatives have a role to play. With regards to the Budapest Convention on Cybercrime Mr. Gercke mentioned that it covers all the main and relevant areas of cybercrime legislation (including substantive criminal law, procedural law, and international cooperation) and can be applied to both common law and civil law countries. He also noted that there is clear difference between using the convention as a reference and actually being a signatory to the convention, as when a country decides to sign the convention they will become part of the committee dedicated to further developing the convention to fit the changing cyber-threat environment. Mr. Gercke further noted that finding adequate solutions to respond to the threat of cybercrime is a major challenge for developing countries. Developing and implementing a national strategy for cybersecurity, including fighting cybercrime, requires time and can be quite costly, which in turn may prevent countries from taking the necessary steps. It is however increasingly important for each country to develop the

[28] http://www.itu.int/ITU-D/cyb/events/2008/brisbane/docs/gercke-legal-foundation-fundamentals-brisbane-july-08.pdf

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

capabilities and competences required to revise their legislation, investigate abuse or misuse of networks and ensure that criminals who attack or exploit the networks are punished.

46. Anthony Angelo, Professor, Victoria University of Wellington, New Zealand, with his presentation "Overview of Cyber-Legislation in the Pacific Islands"[30] provided an insight into the legal tools that are being used in the Pacific Islands to address cybercrime. Mr. Angelo gave a brief overview of cybersecurity laws in the countries of the South Pacific, considered some of the main model laws and legislative examples available to Pacific countries as they seek to deal with cybersecurity matters, and discussed the appropriate approach to deal with the specific needs of Pacific countries. Mr. Angelo noted that there is very little legislation in place in this area in the South Pacific. Most countries would rely, if the issue were to arise in court, on their general criminal laws and particularly those relating to damage to property. There are also some provisions in legislation relating to civil aviation and broadcasting which could be called in. New Zealand, Australia, Kiribati and Tonga do have some specific legislation. Mr. Angelo noted that The Commonwealth had responded to the Council of Europe Convention on Cybercrime in 2002 by preparing two model laws for the use of Commonwealth countries. These drafts are the Computer and Computer Related Crimes Act and the Electronic Evidence Act. These are succinct, clearly presented, and speak directly to the systems of small Commonwealth common law countries. They are probably the best available examples for the countries of the South Pacific, the next best would be the Tongan Act. All reflect the Council of Europe/Budapest Convention on Cybercrime.

47. The focus in the Pacific Ocean area however needs to be specifically calibrated to the Pacific situation. It is equally clear given the ubiquity of electronic communication, that no one country can solve the problems alone. Mr. Angelo highlighted that the major regional planning document – the Pacific Plan of the Pacific Islands Forum – has very little to say about telecommunications and nothing about cybersecurity. The Pacific Plan has for some years been the focus of regional diplomatic endeavors of the Forum Secretariat and the intention is that it will continue to be so for many years to come. It is seen as a blueprint for future regional activity and as a living document. At the regional level, if cybersecurity is to be assured at a national level, cybersecurity should find a place as a priority item in the Pacific Plan, Mr. Angelo recommended. In the absence of regional coordination, Mr. Angelo encouraged country representatives from Pacific Islands present at the meeting, to move ahead as quickly as they can with their anti-spam legislation and cybersecurity legislation. Ultimately momentum will grow on the regional level and there will be regional coordination and cooperation as other countries put their policies in place he said. Every step forward is an important one.

48. Adrian McCullagh, Professor, Telecommunications & Secure E-Business Law, Information Security Institute, Queensland University of Technology, Australia, continued with "Cyber Crime and Information Security: A Legislative Regime"[31]. He started his presentation by looking into the legislative measures that have been put in place in Australia to promote a culture of cybersecurity noting that the Australian Federal Government in recent years has undertaken a number of steps to move forward on this. These steps have included: the establishment of a Trusted Information Sharing Network that comprises various parties and industry associations directly involved with Critical Infrastructure; the enactment in 2001 of the Cyber Crimes Act which substantially improved the legal basis covering cyber crimes; the extension of the Privacy Act in 2001 to cover more private organizations that hold personal information; and the enactment of the Federal Criminal Code especially division 12 which covers Corporate Culture of Non-Compliance with Federal, State or Territory Laws.

49. Mr. McCullagh also mentioned the recently published Security Breach Disclosure Guidelines by the Australian Privacy Commissioner. He brought two of the difficulties in developing a national cybersecurity approach in Australia to the participants' attention. Due to the Federated Environment, Mr. McCullagh explained the Federal Government must operate within the scope of the Australian Constitution which at time can be restrictive in developing a national approach. At the same time in many industry sectors covering critical infrastructure, the relevant infrastructure is owned by private organizations. For example, the banking system, the telecommunications infrastructure, and most transport is either privately owned or operated by Government Owned Corporations. He also highlighted the differences between Australian states; in some states, for instance, the electricity network is privately owned, whilst in other states it is owned by Government Owned Corporations. Fortunately, he said, the Commonwealth does have legislative power to regulate some industry sectors like banking and telecommunications.

50. When Mr McCullagh brought Security Breach Guidelines into the discussions in this session he highlighted that the guidelines only apply where personal information is the subject of the breach and that no civil liability applies. The approach he described substantially follows the Canadian approach, which in turn is partially based upon the Californian enactment of 2003, and furthermore based on what he called the "Shame Factor". As an example he mentioned that in the United States state of California notices to the Secretary of Commerce for California are made public via a web site. In concluding his presentation, Mr. McCullagh noted that laws and legislation are still developing in this arena. He also noted that privacy could be a substantial issue in raising awareness for a security culture, and provided as food for thought the idea that data breach disclosure could be an answer to some of the questions raised in this domain, but that it was still too early to tell.

---

[30] http://www.itu.int/ITU-D/cyb/events/2008/brisbane/docs/angelo-cyber-legislation-in-the-pacific-brisbane-july-08.pdf

[31] http://www.itu.int/ITU-D/cyb/events/2008/brisbane/docs/mccullagh-legislative-regime-brisbane-july-08.pdf

Session 5: Management Framework for Organizing National Cybersecurity/CIIP Efforts and Country Case Studies: Incident Management Capabilities

51. Session 5 looked closer at the different building blocks needed to develop effective Incident Management Capabilities, with examples from countries in the region and beyond. The moderator of this session, Michael Lewis, Deputy Director, Q-CERT, Qatar, opened the session with a presentation on "ITU Incident Management Capabilities Pillar Fundamentals and Qatar Country Case Study"[32], providing an overview of Q-CERT structure and activities, the reason for Q-CERT's being, and how these can be linked to the ITU Management Framework pillar dedicated to developing incident management capabilities. A key activity for addressing cybersecurity at the national level is preparing for, detecting, managing, and responding to cyber incidents through the establishment of watch, warning and incident response capabilities. Effective incident management requires consideration of funding, human resources, training, technological capability, government and private sector relationships, and legal requirements. Collaboration at all levels of government and with the private sector, academia, regional and international organizations, is necessary to raise awareness of potential attacks and steps toward remediation. Among other things, Mr. Lewis noted that countries are asked to consider developing a national cyberspace incident management program in coordination with the intelligence and law enforcement communities as well as participate in watch, warning, and incident response information sharing mechanisms.

52. Mr. Lewis mentioned that Q-CERT, through its growing number of activities, aims to; provide accurate and timely information about current and emerging cyber threats and vulnerabilities; respond to significant threats and vulnerabilities in critical infrastructures by conducting and coordinating activities needed to resolve the threats; serve as a central, trusted partner in security incident; undertake reporting and analysis; promote and facilitate the adoption of standards, processes, methods, and tools that are most effective at mitigating the evolving risks; provide unbiased information and training to build the management and technical skills needed for organizations to effectively manage their cyber risk. Mr. Lewis also explained the role of Qatar's Cyber Security Network, an initiative created to bring together the critical sector organizations in Qatar and the region, to better understand their information security requirements and to enable Q-CERT to focus its output to meeting these needs.

53. Kitisak Jirawannakool, Computer System Officer, ThaiCERT, National Electronics and Computer Technology Center (NECTEC), Thailand, followed with an introduction to the activities of Thailand's ThaiCERT in his presentation "ThaiCERT Incident Response & Phishing Cases in Thailand"[33]. Mr. Jirawannakool explained ThaiCERTs role as the national CERT and some of the products and services that ThaiCERT is providing its constituency with. ThaiCERT was established in 2001 and its main mission is to respond for computer security's incidents within the Thai's government sector. In addition to several dedicated activities within the incident response process, ThaiCERT also works with the Thai army to test security-related equipment. With the growing number of Thai internet users, he noted that in 2007 there were almost 40 million internet users in Thailand, Thailand is seeing internet related treats spreading rapidly. Due to this, ThaiCERT is now also providing services to other parties outside the government.

54. Some of the public services that ThaiCERT provides include user security awareness raising through the publication of security information on the website and a Safety-Net Booklet, and the team also provides e-learning on computer security. When it comes to direct incident response, virus alerts and a security advisory are shared through different channels. Mr. Jirawannakool highlighted that ThaiCERT currently receives quite a big number of incident reports which it tries to manage and respond to within their limited resources. In this regard, the presentation also looked into some of the relevant incident statistics of incidents, categorized by types of incidents and source of attackers. Mr. Jirawannakool mentioned that recently what ThaiCERT has been seeing is that the trend in the number of phishing cases in Thailand has been increasing dramatically.

55. Vu Quoc Khanh, Director General, VNCERT, Viet Nam, in his incident management capabilities country case study for Viet Nam, "Establishing National Incident Response Capability for Viet Nam – VNCERT Activities and Challenges"[34], discussed the current and future activities of VNCERT and highlighted some of the main challenges faced when establishing national incident response capability for Viet Nam. Mr. Khanh started his presentation with an overview of the cybersecurity situation in Viet Nam, the reasons underlying the establishment of VNCERT, its mission and duties and activities undertaken in Viet Nam for improvement of the legal environment. He also gave examples of some of the current incident response and cybersecurity awareness raising activities, emphasizing the importance of increased cooperation and participation in extended national as well as international coordination networks for increased cybersecurity. Mr. Khanh shared information on planned and ongoing research and security specialist training initiatives that VNCERT was undertaking and shared information on the development of a R&D project for setting up a network security monitoring system and the establishment of a national cybersecurity technical center in Viet Nam.

---

[32] http://www.itu.int/ITU-D/cyb/events/2008/brisbane/docs/lewis-Q-CERT-incident-management-brisbane-july-08.pdf

[33] http://www.itu.int/ITU-D/cyb/events/2008/brisbane/docs/jirawannakool-thaicert-brisbane-july-08.pdf

[34] http://www.itu.int/ITU-D/cyb/events/2008/brisbane/docs/khanh-VNCERT-overview-brisbane-july-08.pdf

56. Some of the main challenges that Mr. Khanh sees in developing capacity in this area relate to the lack of legislation and enforcement, lack of technical cybersecurity facilities, human resource shortages, and budget limitations. In order for a country like Viet Nam and an organization like VNCERT to move forward in this challenging area, there is a need for someone to take a leading role in researching and drafting legal and policy documents, establishing an extensive security R&D program and overall ensuring a coordinated approach in implementing the activities. This together with international cooperation and collaboration is a one possible way forward.

57. Graham Ingram, General Manager, AusCERT, Australia, in his presentation on "Incident Management Capabilities – Australia Country Case Study"[35] introduced AusCERT, which is Australia's national CERT. AusCERT has already existed for 15 years and thus is one of the world's oldest CERTs. Mr. Ingram gave examples of how the nature of cyber-attacks have changed over the years and why this has also changed incident management and response. He noted that online identity theft, the act of capturing via the internet another's credentials and/or personal information with the intent to fraudulently reuse it for criminal purposes, the number one threat to E-government and E-business, while state sponsored attacks and terrorism are slowly growing in magnitude. If people think things are bad now, he continued, things are very likely to get much worse. It is difficult to secure what we have now, but it will be increasingly difficult to secure what we will have in the future with Facebook, MySpace, peer to peer networking, etc. growing rapidly. Most users do not know that they have been attacked or are under attack. There are clearly a lot of challenges ahead of us in this are, Mr. Ingram highlighted, and there will be a lot of new job opportunities for security professionals going forward.

58. In responding to overall growing number of threats, the role of a national CERT is very different from other CERTs in a country, especially in areas such as cooperation and coordination. The activities that AusCERT engage in range from monitoring and providing advice about threats and vulnerabilities, incident response and mitigation assistance for ongoing attacks to performing analysis of attacks and malware to understand the nature of the threat, and central coordination and collation of data in order to develop metrics on how the threat is changing. In the CERT world you do not exist if you do not have a network of contacts. Mr. Ingram emphasized that you need to know who to contact and what they can help you with. Thus the need for a trusted network is critical to the work of CERT. Some key requirements moving forward were highlight by Mr. Ingram in this respect. He mentioned the need for better detection mechanisms to identify and track attacks, shared knowledge of attack methodologies and trends, more rapid cross border incident response, better overall understanding of mitigation approaches, better access to quality data for analysis and assessments, and more capacity to deal with CERTs, industry (including vendors and ISPs), government and law enforcement. As an immediate response that can be taken by the parties involved, Mr. Ingram highlighted some takeaways which included the need for more resources nationally and internationally to undertake initiatives that will improve cybersecurity and prevent and mitigate impact of cybercrime, and the need for a better understanding of the nature of the cyber-threats and related vulnerabilities by those assessing risk.

Session 6: Management Framework for Organizing National Cybersecurity/CIIP Efforts and Country Case Studies: A National Cybersecurity Strategy

59. Increasingly, electronic networks are being used for criminal purposes, or for objectives that can harm the integrity of critical infrastructure and create barriers for extending the benefits of ICTs. To address these threats and protect infrastructures, each country needs a comprehensive action plan that addresses technical, legal and policy issues, combined with regional and international cooperation. What issues should be considered in a national strategy for cybersecurity and critical information infrastructure protection? Which actors should be involved? Are there examples of frameworks that can be adopted? Session 6 dedicated to the development of a National Cybersecurity Strategy sought to explore in more detail various approaches, best practices, and the key building blocks that could assist countries in establishing national strategies for cybersecurity and CIIP.

60. Building on the presentations made earlier in Sessions 2, 3, 4, and 5 of the forum that showcased the different pillars of the framework for cybersecurity and CIIP and different national strategies and approaches, Jason Ashurst, Director, ITU and Treaties Section, International Branch, Department of Broadband, Communications and the Digital Economy (DBCDE), Australia moderated this session which describes the final element of the Framework, which ties the other components together, namely the development of a national cybersecurity strategy.

61. The first presentation in this session was delivered by Sabeena Oberoi, Assistant Secretary, Department of Broadband, Communications and the Digital Economy (DBCDE), Government of Australia, on "Australia's Cybersecurity Strategy"[36]. In her presentation, Ms. Oberoi emphasized the need for an overall holistic and integrated approach to cybersecurity, noting that the E-security national agenda is the policy framework for cybersecurity in Australia. The agenda was established in 2002 and reviewed in 2006. The review identified three key priorities stemming from the fact that all things have to be looked at together: Reducing the e-security risk to Australian Government information and communications systems; Reducing the e-security risk to

[35] http://web.itu.int/ITU-D/cyb/events/2008/brisbane/docs/ingram-auscert-casestudy-brisbane-july-08.pdf

[36] http://www.itu.int/ITU-D/cyb/events/2008/brisbane/docs/oberoi-australia-security-activities-brisbane-july-08.pdf

Australia's national critical infrastructure; and Enhancing the protection of home users and SMEs from electronic attacks and fraud. Ms. Oberoi mentioned that another review of the e-security framework is currently being undertaken, but that this review is a bit different in that an entirely new framework might be foreseen due to the ever-changing online environment. She noted that the possible new framework needs to be focused around the most vulnerable sector in this regard, in other words the home users and SMEs.

62. More work for instance needs to be done by the government in collaboration with the private sector and the civil society to targeted awareness raising initiatives. Australia's Stay Safe Online[37] initiative is one effort in this direction, with the "stay smart online alert service" being another one. Ms. Oberoi concluded her presentation by emphasizing the need for increased international cooperation in the area of cybersecurity. A lot of work by different organizations is being undertaken in this area, however, as this is a truly global problem, all countries need to enhance their collaboration with other economies and with organizations such as the ITU, OECD and APECTEL.

63. Michael Lewis, Deputy Director, Q-CERT, Qatar provided an overview of the ongoing and planned initiatives in Qatar, through ictQATAR and Q-CERT activities, in establishing a national cybersecurity strategy in his presentation "National Cybersecurity Strategy – Qatar"[38]. In obtaining agreement on the development of a national cybersecurity strategy, Mr. Lewis mentioned that it is important to create awareness at the national policy level about cybersecurity issues and the need for focused national action and increased international cooperation in this regard. He brought up the need to ensure that all stakeholders, including the decision makers, understand that a national strategy to enhance cybersecurity is needed to reduce the risks and effects of both cyber and physical disruptions. In addition to this, any national strategy needs to be complemented with the participation in international efforts to promote national prevention of, preparation for, response to, and recovery from incidents. With Q-CERT activities maturing, Mr. Lewis said that what is now needed is a group of partners, a CERT for the Gulf Cooperation Council (GCC) countries, to be able to better collaborate, share information and national experiences. He noted that excellent opportunities exist to collaborate with partners in developing a culture of cybersecurity.

64. Mr. Lewis continued his presentation with a practical example of how the ITU Cybersecurity Framework and National Cybersecurity/CIIP Self-Assessment Toolkit can be used by countries to assess where they are at in the development of their national cybersecurity efforts, and where more work is needed going forward. Mr. Lewis mentioned that Q-CERT has found that mapping capabilities onto the Framework was useful to them and in relation to this the development of metrics to measure progress. This initial work in this area was done earlier in 2008 in conjunction with an ITU Regional Cybersecurity Forum in Doha. When discussing strategy and especially a national strategy for cybersecurity, flexibility is crucial. The country needs a clear plan but more often than not reality sets in and what happens during the actual implementation of the strategy needs additional attention. Due to this, in implementing the cybersecurity strategy, the results you see may end up being different from what you initially had in mind. You may find that you are in a better position than you had planned for, but you may also notice that you need to step back and adjust your activities. When developing and implementing a national strategy, many lessons learned are obvious in hindsight. Therefore, it is even more important to learn from best practices and the experiences of others. Mr. Lewis said that the ITU Cybersecurity Framework and related tools provide a structure for thinking through the issues related to the creation of a national strategy. In conclusion, Mr. Lewis pointed out that even the best of strategies is worthless unless the organization has the right people to implement it. Recruiting, training and retaining the right people are therefore critical components in the implementation of any national cybersecurity strategy.

65. Richard Hipa, Managing Director, Niue Post & Telecommunications, Niue Island, in his presentation "Country Case Study – Cybersecurity Related Initiatives in Pacific Island Countries"[39] provided an insight into cybersecurity from a small island perspective. He brought forward some of the special characteristics of the island states that make their needs and requirements slightly different when it comes to addressing cyber-threats and building cybersecurity capacity. When it comes to internet services, these are currently provided to Niue Island by the Internet Users Society Niue (IUSN), and internet access is mainly provided via WiFi and dial up, with WiFi currently available to 75 per cent of villages in Niue. But the relative number of users is still small with the number of internet customers totaling approximately 450, including approximately 250 in government services. Mr. Hipa noted that children start with computer classes in year 5 in primary school and IT is a compulsory subject in the Niue High School. Through a UNDP ICT4D E-Government Project, Mr. Hipa continued, all government departments and corporations previously running their services using WiFi have now been transferred to the government broadband services for increased security and in order to improve efficiency in government services.

66. Despite the low number of users, spam is a severe problem in Niue. The government sees a clear need to formulate some national spam legislation and enhance enforcement and cooperation in this regard. As a result, a joint initiative between the Australian Department of Broadband, Communications and the Digital Economy, and

---

[37] http://www.staysafeonline.gov.au

[38] http://www.itu.int/ITU-D/cyb/events/2008/brisbane/docs/lewis-qatar-national-strategy-brisbane-july-08.pdf

[39] http://www.itu.int/ITU-D/cyb/events/2008/brisbane/docs/hipa-niue-casestudy-brisbane-july-08.pdf

the Australian Aid Agency (AusAID) has been launched. The project, which also includes Samoa and Vanuatu, is being coordinated by DBCDE and Galexia, funded in part by AusAID's Pacific Governance Support Program, and aims to improve the capability of Pacific Island countries to engage in e-commerce and maximize the potential for and development of a consistent legislative and regulatory approach in the Pacific region. More specifically, the project hopes to enable Pacific nations to act against spam both domestically and internationally, and reduce the potential for the establishment of spam 'havens' in the region that undermine global efforts to minimize spam.

67. Phillip Toye, Senior Advisor, Ministry of Economic Development, New Zealand, shared "New Zealand's Digital Strategy 2.0: Smarter Through Digital"[40] with the forum participants. He noted that New Zealand had released its Digital Strategy in 2005 as a response to developments in ICTs and that its vision was for New Zealand to become a world leader in using information and communication technology to realise its economic, social, environmental, and cultural goals, to the benefit of all its people. The three enablers in this strategy were connection, content and confidence. The confidence enabler in this respect included several actions aimed at promoting a more reliable and secure telecommunications and internet environment such as the passing of anti-spam legislation, the development of an e-crime strategy, a national computer security education campaign undertaken by Netsafe and overall ongoing support for the work of Netsafe. The Digital Strategy 2.0 is now an opportunity to assess New Zealand's progress and reset its digital goals for the next five years. Mr. Toye noted that the Digital Strategy 2.0 is currently being finalised, following a lengthy consultation process, and is due for release in August 2008.

68. To get to this stage the country has undertaken a number of related activities. In 2006, for instance, the Ministry of Economic Development released a Discussion Paper entitled "A Strategic Consideration of ICT Security and Confidence in New Zealand". The purpose of the paper was to take a strategic look at ICT security and safety issues in New Zealand and seek feedback in order to assess key gaps and priorities. Guidance was obtained from the OECD work on information security. Some of the key gaps and priorities identified for New Zealand were mainly related to the need for improvement in New Zealand's threat prevention, detection and response capability for critical infrastructure and business networks, the possible creation of a New Zealand CERT, the need for more comprehensive education and awareness-raising for business and households on ICT security and safety risks and protection, and the need for more effective collaboration between government, business and community groups to bring about improved ICT security outcomes. The feedback from the discussion paper has contributed to the work on Digital Strategy 2.0. The new strategy will as a result put forward four priorities for action for the "confidence" pillar. These are a) Ensure the security of ICT infrastructure and networks; b) Enhance the security of digital information; c) Ensure universal awareness of online safety, security and privacy issues; d) Enforce cyber-crime law.

Session 7: Review and Discussion: Management Framework for Organizing National Cybersecurity/CIIP Efforts

69. Session 7, the final session of the day, sought to review and further discuss the pillars that make up the *Management Framework for Organizing National Cybersecurity/CIIP Efforts*, identifying some of the main takeaways from the presentations on the pillars and the related country case studies in preparation for the concluding forum session. To help organize the session, the session moderator, Joseph Richardson, Consultant, United States of America, asked five panelists to give their main takeaways from sessions already held and, if possible, provide some proposals and recommendations for practical next steps in the region.

70. Johannes Bauer noted the importance for all countries to develop a national cybersecurity strategy. While there is nothing that is the best in the world and that will solve all issues straight away, governments and other stakeholders need to try to take clear steps in the right direction. Security is a public good and it needs to be enforced and implemented on the global scale. The weakest link will always determine the overall state of security. Therefore, what is needed is a global and international approach that ties all different initiatives together. Mr. Bauer further noted that while the technologies are the same, the challenges that countries are facing when it comes to the implementing cybersecurity initiatives are not identical. This needs to be considered in any approach taken. In the end, he concluded, security is expensive, and not only public funding should be going towards building a secure online environment. There is an urgent need to think about the financial implications of implementing security for the different stakeholders and players, and thus a need to look at the costs that the different players are forced to carry.

71. Keith Besgrove noted in his remarks that Australia has been able to develop quite a comprehensive national e-security strategy and related framework but it has taken Australia eight years to get where it is today. He also mentioned that some level of competition between national agencies is good in developing a strategy and that the international component of any national cybersecurity strategy is critical. Here he emphasized the usefulness of extensive regional engagement and collaboration. In concluding, Mr. Besgrove drew the forum participants to the fact that there are still no direct laws for the internet. What is needed, he said, is to change

[40] http://www.itu.int/ITU-D/cyb/events/2008/brisbane/docs/toye-new-zealand-strategy-2.0-brisbane-july-08.pdf

the price signals on the internet and alter people's behavior. This, together with encouraging a better standards focus, is the best way to move forward.

72. Marco Gercke brought the participants' attention to the fact that even if countries take on different approaches to addressing cybersecurity challenges, at the same time these countries are closely connected. He noted that there are a number of international initiatives for cybersecurity and the fight against cybercrime, and that all these different initiatives have a role to play. An effective fight against cybercrime requires global harmonization of criminal laws and criminal procedural laws, the application of standards, together with international cooperation.

73. When looking at developing a national cybersecurity strategy, all stakeholders need to be involved in this effort, directly or indirectly. Richard Beach asked countries to remember to include agencies that are not necessarily government agencies when formulating national cybersecurity plans and strategies. Also do not forget the safety and security of children and young people when formulating plans and strategies for your countries, Mr. Beach recommended. When trying to comply with a global model, Mr. Beach continued, it is important not to sacrifice a country's own culture in the process.

74. Joseph Richardson noted in his comments that he had heard some good reasons during the course of the past few days why governments should work with industry for cybersecurity and noted that there are many different ways in which to collaborate with the industry. In all countries we face the issue that everyone in industry, all different sectors and enterprises, cannot be engaged. To deal with this, countries need instead to find an approach that gathers these representatives in industry associations that in turn can debate on their behalf. Further work is needed to define the frameworks required for this collaboration. Industry collaboration also needs to be looked at in different ways. In particular one area that needs to be further developed is the role of relationships, not only with industry but also with other elements of government. In the future we need to ensure that other ministries, in addition to the communications ministries, are involved in the cybersecurity fora, workshops and related activities.

Sessions 8 & 9: Cybersecurity and Small Island Developing States (SIDS)

75. Sessions 8 and 9 of the forum aimed to provide more information on and discuss in further detail the needs and special requirements of Small Island Developing States (SIDS) and Pacific Island countries due to unique challenges posed by their small size and remoteness. The sessions reviewed some of the ongoing initiatives in the Pacific and tried to elaborate on a possible cooperation model going forward. Ivan Fong, Vice-President, Pacific Islands Telecommunications Association (PITA) acted as the moderator for Session 8 and Stuart Davies, representative for Asia-Pacific Telecommunity (APT) as the moderator for Session 9.

76. Daniel Wells, Assistant Director, Department of Broadband, Communications and the Digital Economy (DBCDE), Australia, in his presentation "Australian Government Cybersecurity Activities in the Pacific"[41], among other initiatives, provided an overview of the Anti-Spam Legislation Project. He noted that when it comes to the engagement with the Pacific Islands DBCDE plays a key coordinating role, working together with partners such as ITU, APT, APEC, Pacific Islands Telecommunications Association (PITA), and the Pacific Island Forum Secretariat (PIFS) on a number of different activities geared towards assisting policy makers and regulators through capacity building projects to improve access, security and governance in the telecommunications sector. Cybersecurity is one of the key work areas for the Pacific which is coordinated across the main regional and international organizations through different initiatives. The World Bank regional resource centers were also mentioned as an important cornerstone in these activities. Mr. Wells gave an example of the Anti-Spam Legislative Project which aims to strengthen spam legislation, enforcement and cooperation regimes in the Pacific for island countries. Currently Niue, Samoa and Vanuatu are involved in the project with support from AusAID and the Australian Communications and Media Authority (ACMA). Legislation is at various stages in the participating island states and lessons learned from similar earlier work in Tonga and the Cook Islands are therefore also taken into consideration in this effort.

77. Mr. Wells further noted that there are three parts to the project, which is modeled around the Australian approach and Spam Act. This includes developing anti-spam legislation specific to each country using Australia's Spam Act as a model, building local enforcement capacity, and participating in international law enforcement networks. One of the challenges the region is faced with, he continued, is the small number of people that the countries can dedicate to specific initiatives of this kind. Immediate steps forward in the implementation of the project include identifying and sharing awareness raising and education materials, allow the PICs to review their legislation, and increase PICs' participation in international anti-spam fora. In his presentation, Mr. Wells also brought up the plans to move forward on the establishment of a Pacific CERT that had mentioned by Minister Conroy in his address earlier in the forum. The reasons why the region would benefit greatly from the initiation of a regional CERT, include but are not limited to, being able to provide a coordinated approach to informing key stakeholders of the latest cyber-threats, assist in developing coordinated responses to these threats, and the possible pooling of scarce resources both in terms of people and funds. The CERT function is furthermore an important part of a broader national cybersecurity strategy.

[41] http://www.itu.int/ITU-D/cyb/events/2008/brisbane/docs/wells-australian-initiatives-in-pacific-brisbane-july-08.pdf

78. Franck Martin, ICT Specialist, The Pacific Islands Applied Geoscience Commission (SOPAC), and Chairman, The Pacific Islands Chapter of the Internet Society, Fiji, shared his views on the current "Pacific Cybersecurity Environment"[42]. Mr. Martin noted that as he has been involved in installing servers in each country in the Pacific he has been able to get an idea about what the current situation is, and what some of the specific challenges are with regards to connectivity and deployment of ICTs in the Pacific region. One of these is the fact that there is no "line of sight" which makes it difficult to connect to the islands. This, in addition to the lack of service level agreements with the service providers also creates problems when it comes to commitment and services provided to the islands. There are also general problems with regards to capacity building in the ICT area. In the area of cybersecurity, Mr. Martin noted that currently sending spam is not an illegal activity in the Pacific Islands. A user, if inclined to do so, can send out a million e-mails and will not face any problems while doing so. A number of activities, in addition to the Australian Anti-Spam project that was mentioned earlier by Mr. Wells, have been initiated on the islands. These are often very informal activities that are driven by not-for-profit organizations.

79. An example is an information-sharing network of young professionals from the islands who are communicating through a forum on Skype. This seems to be an approach that is working really well, Mr. Martin continued, and emphasized the need to use new communication tools to get people more engaged. In this regard Mr. Martin further brought up the discussion regarding the role of a Pacific CERT and how the CERT could potentially build on this initial network of professionals, to first and foremost share experiences and information, and also more confidential information. He noted though that the process of setting up a CERT is not only about building and setting up networks but also about applying standards and procedures to these. When asked about what aspects of best practices that do not seem to work for the Pacific Islands, Mr. Martin noted the need to start small and then add the necessary extra steps and bring people in slowly.

80. Stuart Davies, previous Chief Executive and Managing Director, Telecom Cook Islands Ltd and now Representative for Asia-Pacific Telecommunity (APT), presented on the case of "Telecom Fraud and Number Hijacking"[43] and the impact this has on the Pacific Islands. Mr. Davies noted that number hijacking is one of the key security issues affecting the Pacific, highlighting that hijacking also has a fraudulent twist to it. There are apparent regulatory, policy, and standards gaps in this area that need to be addressed with a sense of urgency. He was talking mainly about hijacking within the internet protocol space, while noting that hijacking at the DNS and ENUM level is also something that can happen. Pacific Island administrations are well aware that the unauthorized hijacking of number ranges and country codes of some Pacific Islands and the use of these numbers for International Revenue Share Fraud (IRSF) and fraudulent activities is occurring. Hijacked calls, Mr. Davies noted, are calls that do not terminate in the Pacific Island country because some-one, for fraudulent reasons, has filtered the calls away from the routing to the intended country. This in turn gives rise to additional roaming charges involving losses of hundreds of thousands of dollars.

81. Other fraudsters, he continued, filter the calls to porn sites without the knowledge of the home operator to collect the terminate rate. This has caused some operators to block calls to the Pacific Islands to avoid getting caught by the fraud and thus affecting the inhabitants in the countries directly. Mr. Davies drew the participants' attention to what they need to do to respond to this challenge. The APT will in the coming month send out to government member administrations voting papers to seek the approval of members to forward the various Preliminary APT Common Proposal (PACPs) (about 28 in total) as a Common Proposal to go to the ITU World Telecommunication Standardization Assembly (WTSA) held in October 2008. He noted that members must vote for the Common Proposal if it is to succeed. If the proposal gets enough support, then it will go to the ITU WTSA as an APT Common Proposal. Mr. Davies was further encouraging Pacific Islands who are a member of ITU to attend the upcoming WTSA to back the possible proposal.

82. Glennys Vora, Information Systems and Services Unit (ISSU), Department of Finance, Republic of Vanuatu, in her Country Case Study[44] on cybersecurity-related initiatives in Pacific Island countries shared with the forum participants some of the cybersecurity activities that are taking place in Vanuatu. While noting that Vanuatu has no integrated national ICT policy at this point in time she highlighted that there are a number of initiatives in place that are able to support the security requirements of government information technology network operations and the limited government portals that are used for financial and commercial information. Ms. Vora mentioned that the government, through the Ministry of Infrastructure and Public Utilities, is now developing a new Sector Policy for Telecommunications/ICT which aims to enhance the country's competitiveness and growth prospects.

83. In order to make Vanuatu's enterprises more efficient and the country more competitive overall, the government understands that the private sector needs to be more actively engaged in order to successfully implement these and other more direct cybersecurity goals. Vanuatu has made a lot of progress over the past 12 months with its efforts to put in place the necessary legislations and policies for overall ICT development in order to provide a secure foundation for the information society and create an environment that is favorable and

---

[42] http://www.itu.int/ITU-D/cyb/events/2008/brisbane/docs/martin-pacific-islands-overview-brisbane-july-08.pdf

[43] http://www.itu.int/ITU-D/cyb/events/2008/brisbane/docs/davies-number-hijacking-brisbane-july-08.pdf

[44] http://www.itu.int/ITU-D/cyb/events/2008/brisbane/docs/vora-cybersecurity-initiatives-vanuatu-brisbane-july-08.pdf

competitive to investments and partnerships in ICT. The country has, for instance, been working actively on the drafting of anti-spam legislation together with the Australian government and other countries in the region. Going forward more work is required to finalize the draft legislation.

84. Tua'imalo Asamu Ah Sam, Chief Executive Officer, Ministry of Communications and Information Technology, Independent State of Samoa, shared the "Samoa Case Study"[45] with the forum participants. Countries big and small need to consider cybersecurity very seriously. As the islands have very limited resources, Mr. Ah Sam continued, they are very dependent on assistance from donor countries. Samoa as an independent state with a population of around 180,000 people has recently undergone the process of telecommunication reforms and has as a result separated telecoms policy, regulations and operations. With four main ISPs active in the country (Computer Services Ltd, I-Pasifika, Lesamoa.net, and Samoatel), the country currently have approximately 7500 internet users. This low number, Mr. Ah Sam noted, is mainly due to the high cost of acquiring a PC and the lack of basic access. Mobile phone coverage is currently around 95 per cent, but expensive.

85. Spam is a problem that has been receiving increasing attention in the country and the ISPs are putting in extra filters to block off this spam. Samoa has also participated in the anti-spam legislative project that was mentioned by DBCDE in one of the earlier presentations. Mr. Ah Sam mentioned mobile phone spam as an emerging issue related to this that the country is starting to see. He noted that he has learned a lot about cybersecurity at this regional forum and that he would now go back to Samoa to try to do more in this very important area.

86. As the last Pacific Island country to present on their activities, Igam Moaniba, Republic of Kiribati presented on the "Kiribati Country Case Study"[46]. He gave an insight into the telecommunications environment in Kiribati and the status of cybersecurity. Cybersecurity he noted is not considered highly important by most people as well as the government as the majority of people are not aware of the seriousness of cybercrimes. The reason for this is the absence of online banking, online shopping, and other e-commerce systems and applications, as the main use of the internet in the country is for sending e-mail. The government is currently looking towards cyber-legislation, hoping to establish a national framework and raise awareness on this. The first step in this regards is a multi-stakeholder workshop. That is the beauty of being small, Mr. Moaniba said, the whole island can come to the meeting. Because the country is so small all the different parties can easily come and participate in the meeting. The objective of the planned workshop, which scheduled to take place in the coming 2-3 months followed by consultations between government and private bodies, is to advise stakeholders on the framework and principles related to cyber-legislation, and the various elements of such a framework. This will hopefully raise people's awareness of the issues involved and identify barriers to moving forward on the development and implementation of cyber-legislation.

87. The goal, Mr. Moaniba continued, is to come up with a roadmap for cyber-legislation. The main challenge that the country is currently facing is the lack of knowledge and experience required to draft cyber-legislation and policies, and he invited assistance in this area. The lack of technical skills to be able to identify and counteract cyber related attacks was also highlighted. In order for the country to be able to move forward on a possible action plan in this regard, Mr. Moaniba concluded, the country needs a well-trained workforce, as well as legal and technical assistance.

Session 10: Regional and International Cooperation

88. Regional and international cooperation is extremely important in fostering national efforts and in facilitating interactions and exchanges. The challenges posed by cyber-attacks and cybercrime are global and far reaching, and can only be addressed through a coherent strategy within a framework of international cooperation, taking into account the roles of different stakeholders and existing initiatives. As facilitator for WSIS Action Line C5 dedicated to building confidence and security in the use of ICTs, ITU is discussing with key stakeholders how to best respond to these growing cybersecurity challenges in a coordinated manner. For instance, the ITU Global Cybersecurity Agenda (GCA) provides a platform for dialogue aimed at leveraging existing initiatives and working with recognized sources of expertise to elaborate global strategies for enhancing confidence and security in the information society. This session facilitated by Eun-Ju Kim, Head, ITU Regional Office for Asia and Pacific, reviewed some of the ongoing initiatives in order to inform meeting participants and to further the discussions in order to identify possible next steps and concrete actions to foster and promote international cooperation for enhanced cybersecurity.

89. Keith Besgrove, First Assistant Secretary, Department of Broadband, Communications and the Digital Economy (DBCDE), Australia, and Chair, OECD Working Party on Information Security and Privacy (WPISP) in his presentation "Regional and International Cooperation on Cybersecurity"[47] noted that there is no single multi-lateral organization that can do everything in the cybersecurity area. As a result countries need to be involved in a number of different cybersecurity-related fora. On the regional level, Australia has long been involved in the

[45] http://www.itu.int/ITU-D/cyb/events/2008/brisbane/docs/ah-sam-samoa-casestudy-brisbane-july-08.pdf

[46] http://www.itu.int/ITU-D/cyb/events/2008/brisbane/docs/moaniba-kiribati-casestudy-brisbane-july-08.pdf

[47] http://www.itu.int/ITU-D/cyb/events/2008/brisbane/docs/besgrove-WPISP-brisbane-july-08.pdf

work done by APECTEL in this area and has also found the OECD a useful forum since many of the discussions related to policy issues, analysis, and the preparation of best practices documents start in places like OECD, even though the OECD as such does not have the capacity to be involved in implementation of the different activities in the regions. The OECD Working Party on Information Security and Privacy (WPISP), Mr. Besgrove noted, is one four working groups. Within the working group there is strong emphasis on critical information infrastructure protection as well as identity management, however, not as much focus on identity management and fraud as one might be expecting.

90. Mr. Besgrove mentioned that quite a lot of work has been done on anti-spam measures to date and there are strong commonalities between the pieces of work that have come out of the OECD working groups and the ITU toolkits. What has been seen to work best in elaborating on best practices and trying to come to a common understanding in the area of cybersecurity is when countries get together and work in volunteer groups, as this builds the kind of buy-in that is needed and provides that input required to move forward on the creation of useful deliverables. As an example Mr. Besgrove mentioned the 2002 OECD Guidelines for the Security of Information Systems and Networks a good set of principles for guiding policy development that have been picked up by a number of countries. While it is very important for nation to have national frameworks for cybersecurity, he continued, our laws do not work as well as they should when it comes to the internet and this forces countries to collaborate more internationally. The internet has changed the world forever and everyone is trying to catch up. As the chair of the WPISP, Mr. Besgrove noted that the OECD will continue to look forward to ways in which to collaborate with other parties.

91. Jinhyun Cho, Senior Researcher, Korea Internet Security Center (KrCERT/CC), Korea Information Security Agency (KISA), and Convener, APECTEL Security and Prosperity Steering Group (SPSG), in his presentation on "APECTEL SPSG's International Cooperation Activities"[48] provided an overview of APECTEL's work in the area of cybersecurity. Mr. Cho noted in his presentation that increased international and regional collaboration is needed to address cross-border cybersecurity issues and more effort in the region needs to be placed on narrowing the gap between the cybersecurity readiness in APEC economies. What is required is an approach to cybersecurity that is multi-dimensional, multi-stakeholder (involving government, business, civil society), and international (consisting of coordinated global, regional, bilateral, and multilateral activities) in scope. APECTEL's current approach to cybersecurity is focused around three main pillars of work: cybersecurity, cybercrime, and disaster management, with special attention to the multi-dimensional and multi-stakeholder aspects of this. APECTEL does not have the kind of toolkit that is being drafted in ITU-D Question 22/1, Mr. Cho continued, and therefore this toolkit might also be useful for APEC's 21 member economies.

92. In enhancing cybersecurity, APECTEL has worked on a number of initiatives, with the member states and with other organizations. This has included for instance capacity building on CERT/CSIRT activities through specific watch, warning and incident response awareness raising and capacity building initiatives to strengthen effective response capabilities among APEC economies. Other projects have been dedicated to information sharing and cooperation, policy and technical approaches to take down botnets, security for ICT products and services generally and more specifically security for handheld mobile devices. Mr. Cho ended his presentation by re-emphasizing the need to work together, across borders, to catch the cyber criminals.

93. Stuart Davies, as a representative for Asia-Pacific Telecommunity (APT) provided some additional remarks[49] on the importance of international and regional cooperation to move forward on the issues that have been discussed with regards to cybersecurity. He noted that he was happy to see that many of the organizations active in this area, both on a regional and international level are committing to work together on solutions to the security problems that we are now seeing and that will grow in magnitude in the coming years. He highlighted the importance of sharing information and expertise, and working together, as this gives all parties involved a much greater chance for success. As we have heard in some of the country case studies, the geographical challenges and the nature of the Pacific Islands, makes it even more critical that we work together on the developing and implementing solutions.

Session 11: Wrap-Up, Recommendations and the Way Forward

94. The final session of the meeting was facilitated by Keith Besgrove, First Assistant Secretary, Department of Broadband, Communications and the Digital Economy (DBCDE), Australia and Eun-Ju Kim, Head, ITU Regional Office for Asia and Pacific. Together they reported on some of the main findings from the event, and elaborated on a set of recommendations for future activities in order to enhance cybersecurity and increase protection of critical information infrastructures in the region. Ms. Kim provided a summary of the forum sessions, briefly highlighting the main points of each session. In **Session 1** cybersecurity and critical information infrastructure protection were examined within the context of the ITU National Cybersecurity Framework currently being developed in the ITU Development Sector's Study Group 1 under its Question 22/1-related work. In addition to an insight into the Framework and the related ITU National Cybersecurity/CIIP Self Assessment Toolkit, the participants also learned about some of the issues currently under discussion in Australia with regards to critical

[48] http://www.itu.int/ITU-D/cyb/events/2008/brisbane/docs/cho-apectel-cybersecurity-overview-brisbane-july-08.pdf

[49] No slides available.

infrastructure protection. The address by Senator Stephen Conroy, Minister for Broadband, Communications and the Digital Economy (DBCDE), further highlighted some of the main activities undertaken by the executing agencies in Australia in order to work towards implementing a shared vision of promoting a culture of security as well as building confidence and security in the use of ICTs.

95. **Session 2** followed with promoting a culture of cybersecurity, where we all learned about some of the innovative initiatives in the region that aim to raise awareness of the importance of cybersecurity and educate users of all ages about how they protect themselves and stay safe online. The important and specific roles played by the different actors – i.e. the government, the private sector, academia, civil society in promoting a culture of cybersecurity – were highlighted. **Session 3** focused on building stronger and more effective relationships between government and industry, and we learned about the benefits from engaging industry early, from development to implementation of a national cybersecurity strategy. We also learned about the benefits of Cyber Storm exercises and why this is a useful exercise for both the government agencies and private sector players. **Session 4** talked about the need for appropriate legislation, international legal coordination and enforcement as important elements in preventing, detecting and responding to cybercrime and the misuse of ICTs. Discussions in this session looked at specific aspects of the Council of Europe's Convention on Cybercrime and the challenges faced by Pacific Island nations in crafting cybercrime-related legislation. Different tools and resources available to help Member States to understand cybercrime were also shared.

96. **Session 5** noted that one of the main activities for addressing cybersecurity at the national as well as regional level is preparing for, detecting, managing, and responding to cyber incidents through the establishment of watch, warning and incident response capabilities or CERT/CSIRT type of activities. It was noted that threats to cybersecurity are becoming more severe; and while it is difficult to secure our online assets today, it will be increasingly difficult to secure what we will have in the future. **Session 6** focused on the final pillar of ITU's national cybersecurity framework, the development of a national cybersecurity strategy, and here the forum participants listened to a number of interesting presentations and country case-studies. What happens in bigger countries often filters down and affects also the smaller countries. We learned how the ITU National Cybersecurity/CIIP Self-Assessment Toolkit can be a useful tool and benchmark for both developed and developing economies, when governments review and try to better understand their existing national approach to cybersecurity as well as when they are trying to identify areas for attention, and prioritize to address cybersecurity.

97. In the summary session, **Session 7,** the participants acknowledged that improving cybersecurity is a global problem and that each country must undertake action to join and support international efforts to improve cybersecurity. **Sessions 8 and 9** were dedicated to the special needs and requirements of Small Island Developing States (SIDS) when it comes to enhancing cybersecurity. These two sessions discussed the need for increased capacity building for interested countries in the Pacific region. In conclusion, **Session 10** was dedicated to Regional and International Cooperation. The session highlighted again that regional and international cooperation is extremely important in fostering national efforts and in facilitating interactions and exchanges, at all levels, for increased cybersecurity in the interdependent and globalized information society. The ITU Global Cybersecurity Agenda (GCA) was mentioned as useful guide for raising awareness and initiating and/or reviewing national cybersecurity action as well as ensuring consistency and compatibility at international level. The importance of regional cooperation, joint initiatives and the sharing of resources and information on best practices, training and education was noted as critical going forward.

98. **Six recommendations for concrete action** that need to be taken by countries in the region were identified:

- Identify and provide ITU with a focal point responsible for coordinating with ITU, in particular with the Regional Office for Asia and the Pacific, with regards to cybersecurity-related activities.
- Enhance watch, warning and incident response capabilities in the Pacific Islands through the creation of a Pacific CERT, studying first the ways of creating and maintaining such a Computer Emergency Response Team (CERT)/ Computer Incident Response Team (CSIRT).
- Encourage countries in the region to use the ITU Cybersecurity Framework and related tools as a structure for thinking through issues related to the creation of a national cybersecurity strategy.
- Use available resources, toolkits and material to raise awareness amongst all stakeholder groups on cybersecurity threats as genuine security can only be promoted, when every user is aware of the possible dangers and threats online.
- Share information on national cybersecurity best practices with other countries in the region and play an active role in the activities to finalize the report being developed in ITU-D Study Group Question 22/1: Securing information and communication networks – Best practices for developing a culture of cybersecurity.
- Carry out a study on economic aspects and indicators of cybersecurity.

99. As the way forward, Ms. Kim noted, **ITU is committed to doing the following**:

- At the international level, strengthen collaboration among its three Bureaus and its partners. The Union will also enhance its partnerships with other international organizations including standardization bodies, governments, and private sectors in areas related to cybersecurity and critical information infrastructure

protection and will also continue working closely with its regional offices to assist ITU Member States and Sector Members in related activities.

- At the regional and national levels, ITU's Regional Office for Asia and the Pacific will work in close cooperation with the BDT ICT Applications and Cybersecurity Division to assist Member States especially the developing countries in the Asia-Pacific region in key areas such as: e.g. providing forums for participants to learn about ITU's new products, to gain more knowledge from experts, to exchange information and practices among countries. In this regard, it is expected that a regional forum on cybersecurity will again be organized in the Asia-Pacific region in 2009.
- Continue building human capacity through training programme and workshops. For instance, on-line training and/or face-to-face classroom training will be provided through five ITU Centres of Excellence in the Asia-Pacific region.
- Provide ITU toolkits such as the ITU National Cybersecurity/CIIP Self-Assessment Toolkit, and any other available tools, through close coordination between ITU Regional Office and focal points of the countries.
- Provide ITU experts as part of direct country assistance to help countries implement activities related to cybersecurity such as development and implementation of cybersecurity strategies, cybercrime legislation and enforcement mechanisms.
- Facilitate the establishment of the Pacific CERT and national CERTs in the region.

Meeting Closing

100. In her closing remarks on behalf of ITU, Eun-Ju Kim, Head, ITU Regional Office for Asia and Pacific hoped that the three day ITU Regional Cybersecurity Forum for Asia Pacific, including the one day seminar on the Economics of Cybersecurity, had proven useful for the event participants. Ms. Kim thanked everyone who had directly or indirectly contributed to the success of the forum and relayed special thanks to the local hosts, for their outstanding work in making this Regional Cybersecurity Forum a highly successful event. Ms. Kim also thanked the forum speakers for taking time out of their busy schedules to share their experiences and expertise with the forum participants. ITU with its long standing activities in the standardization and development of telecommunications hopes to continue to provide a forum where the diverse views from governments, the private sector and other stakeholders related to cybersecurity and CIIP can be discussed through its different activities and initiatives.

The email address for comments on this meeting report[50] and for comments on the ITU Cybersecurity Work Programme to Assist Developing Countries (2007-2009)[51], is **cybmail(at)itu.int**[52].

For information sharing purposes, all meeting participants will be added to the **cybersecurity-asia-pacific(at)itu.int**[53] for matters concerning ITU-D cybersecurity-related activities. If you have not participated directly in the event, or are not already on the mailing list but interested in participating in these discussions through the relevant mailing list and forum, please send an e-mail to **cybmail(at)itu.int**.

[50] This Forum Report is available online: http://www.itu.int/ITU-D/cyb/events/2008/brisbane/docs/brisbane-cybersecurity-forum-report-july-08.pdf

[51] http://www.itu.int/ITU-D/cyb/cybersecurity/index.html#workprogramme

[52] Please send any comments you may have on the workshop report to cybmail@itu.int

[53] Regional ITU cybersecurity mailing list: cybersecurity-asia-pacific@itu.int. Please send an e-mail to cybmail@itu.int, to be added to the mailing list.

ANNEX 1

TAS Seminar on the Economics of Cybersecurity

held in Brisbane, Australia on 15 July 2008,

1. The first day of the ITU Regional Cybersecurity Forum for Asia-Pacific, 15 July 2008, was dedicated to an ITU Tariff Group for Asia and Oceania (TAS) Seminar on the Economics of Cybersecurity. During discussions at the previous TAS group meeting held in Seoul, Korea in 3-6 July 2007, TAS Members requested the ITU Development Bureau to organize the next TAS seminar on the economic aspects of cybersecurity, as this issue is becoming increasingly relevant to the countries in the region. The one day seminar was chaired by the chairperson of the Tariff Group for Asia and Oceania, Sahib Dayal Saxena from India.

2. Mr. Saxena and Jason Ashurst, Director, ITU and Treaties Section, International Branch, Department of Broadband, Communications and the Digital Economy (DBCDE), Australia, opened the seminar and welcomed the meeting participants to this first day of the ITU Cybersecurity Forum for Asia-Pacific. Mr. Saxena in his remarks[54] noted that cybersecurity has become one of the major concerns in the closely connected world community, for netizens, entrepreneurs and users of telecom services and ICT alike. It is a question of safeguarding the interests of the world community, where firewalls have to be installed all around infrastructure of communication and, he continued, it seems to be a dilemma that in a world which wants to freely communicate, brick walls and firewalls have to be built. To maintain security of the network for uninterrupted communication among nations and people, the process of security will have to be taken care of. There is also economics involved in building up this security, Mr. Saxena explained. The more we try to create a secure networked environment, the more difficult it becomes to maintain this environment, and the more money is spent. Better solutions will therefore need to be found to build safe and secure connected environment, solutions that cut down the related costs but do not compromise the security of networks. With this Mr. Saxena invited the seminar participants to consider new methods and find innovative solutions to these issues, so that in the world of telecommunications, costs are reduced with no compromise to security.

Seminar Session 1: The Economics of Cybersecurity and The Financial Aspects of Network Security: Malware and Spam

3. The costs and revenues of all stakeholders across the value network of information services, such as software vendors, network operators, Internet Service Providers (ISPs), and users, are affected by malware and spam. These impacts may include, but are not limited to, the costs of preventative measures, the costs of remediation, the direct costs of bandwidth and equipment, and the opportunity costs of congestion. This is further complicated by the fact that spam and malware also create new revenue streams, both legitimate and illegitimate. They enable legitimate business models (e.g., anti-virus and anti-spam products, infrastructure, and bandwidth) as well as criminal business models (renting out of botnets, commissions on spam-induced sales, pump and dump stock schemes, etc.). Consequently, they create mixed, sometimes conflicting incentives for stakeholders, which complicate coherent responses to the problem. This first seminar session provided an introduction to the economics of cybersecurity and reviewed some of the current leading thinking and research in this area, and specifically explored the financial impacts of malware, and the economics of spam. Mr. Saxena from the ITU Tariff Group for Asia and Oceania acted as the moderator for the four seminar sessions.

4. Johannes Bauer, Professor, Michigan State University, opened the first session of the seminar with a background study, "ITU Study on the Financial Aspects of Network Security: Malware and Spam"[55]. The study is a survey of existing resources and data available when it comes to the economics and financial aspects of cybersecurity. As such the report aims to document the state of knowledge of these financial aspects by triangulating the data, to look at the issue from different angles and see if the same answers appear. Measures to improve information security enhance trust in online activities and contribute directly and indirectly to the welfare gains associated with the use of information and communication technologies (ICTs), he explained. However, some expenditure on security is only necessary because of relentless attacks by fraudsters and cybercriminals that undermine and threaten trust in online transactions. Such costs are not welfare-enhancing but instead a burden on society. Two vectors through which such attacks are carried out are malware and spam. Mr. Bauer explained that during the past two decades, the production and dissemination of malware has grown into a multibillion dollar business. Damages created by fraudulent and criminal activities using malware and the costs of preventative measures are likely to exceed that number significantly. Malware puts the private and the public sector at risk because both increasingly rely on the value net of information services.

5. Spam and malware have multifaceted financial implications on the costs and the revenues of participants in the ICT value chain. The costs carried by all stakeholders across the value network of information services, such as software vendors, network operators, ISPs, and users, are affected directly and indirectly by this. Overall,

---

[54] http://www.itu.int/ITU-D/cyb/events/2008/brisbane/docs/saxena-opening-remarks-economics-seminar-brisbane-july-08.pdf

[55] http://www.itu.int/ITU-D/cyb/events/2008/brisbane/docs/bauer-financial-aspects-spam-malware-brisbane-july-08.pdf

malware and spam are associated with a web of financial flows between the main groups of stakeholders in the information and communication value net. Most of the financial flows between the legal and illegal players in the underground cybercrime economy, for example, are not or only partially known.

6. The background study prepared by Mr. Bauer and his team develops a framework within which these financial impacts can be assessed and brings together the many disparate sources of financial data on malware and spam. Some of the findings of report include: a) Estimates of the financial effects of malware differ widely, figures for overall effects range from USD 13.2 billion of direct damages for the global economy (in 2006) to USD 67.2 billion in direct and indirect effects on businesses in the United States alone (in 2005). b) Numbers documenting the magnitude of the underground internet economy and transactions between it and the formal economy also vary widely. One source estimates the worldwide underground economy at USD 105 billion. c) No reliable numbers exist as to the potential opportunity costs to society at large due to reduced trust and the associated slower acceptance of productivity-enhancing IT applications. However, a considerable share of users have expressed concern and indicated that it reduces their willingness to perform online transactions. d) Although the financial aspects of malware and spam are increasingly documented, serious gaps and inconsistencies exist in the available information. This complicates finding meaningful and effective responses, and for this reason, more systematic efforts to gather more reliable information would be highly desirable, Mr. Bauer explained.

7. Marco Gercke, Lecturer, University of Cologne, Germany, then looked in the "The Cost to Developing Countries"[56], asking how much it really costs to improve cybersecurity in a country. Mr. Gercke noted that in some countries you would have to invest more and in other countries less as countries are at highly different levels of development. Given the special situation of developing countries, countries that are right in the middle of a rapid development process, the special needs of these countries need to be taken into consideration when considering the financial investments required to adequately fight cybercrime. Having said this, Mr. Gerck asked: who should be cover the costs related to cybersecurity and especially the cost of cybercrime? Furthermore, the exact amounts needed to do this are not clear, while some say USD 1 billion others say USD 60 billion. If we know how much the related cost is then we would also know how much cost we need to put on the criminals' shoulders. Looking at some of the bigger attacks that we have seen in the recent years, the "I love you virus" for instance did not "cost" anything to develop and launch. At the same time banks are not telling us exactly how much we are losing to cyber-related crimes. Therefore, there is an urgent need for more trustworthy studies into these costs and the government and law enforcement should play a leading role in this regard, Mr. Gercke explained.

8. The internet connects millions of people, and today there are more internet users in developing countries than there are in developed countries. The potential for further growth is great in developing countries but at the same time there is also a growing interest in these growing markets by online offenders. Taking this into account, USD 100 lost by a person in a developing country can have a much more severe impact on a person's life than if a person in a developed country loses USD 10,000. When it comes to potentially covering the cost of cybercrime, Mr. Gercke mentioned that the offender, the victim of cybercrime attack, and industry all end up having to cover part of the costs involved. It is clear that there is a chain of costs involved but in the end it is the user that ends up having to pay higher fees for associated services. Industry has already implemented several technical protection and prevention measures, and the implementation of further obligations is being discussed (e.g. data retention obligation). However, the costs covered by industry are often re-allocated so that in the end the users cover also these costs though fees. The government covers some costs related to the fight against cybercrime by providing law enforcement services. While many banks are compensating their clients who are targets of phishing attacks, and also when it comes to intercept technologies, often the victims cannot get full compensation for financial losses incurred and therefore end up covering the cost. The offenders are in general the ones who have a financial benefit, however, the benefits are not necessary identical to the costs incurred.

Seminar Session 2: The Botnet Economy

9. Botnets are networks of compromised computers infected with viruses or malware to turn them into "zombies" or "robots" — computers that can be controlled without the owners' knowledge. Criminals can use the collective computing power of these externally-controlled networks for malicious purposes and criminal activities, including, inter alia, generation of spam e-mails, launching of Distributed Denial of Service (DDoS) attacks (e.g., for blackmail purposes), alteration or destruction of data, and identity theft. An underground economy has sprung up around botnets, yielding significant revenues for authors of computer viruses, botnet controllers and criminals who commission this illegal activity by renting botnets. While many countries are investing a lot to deal with the problems related to malware and spam, some experts recommend countries to focus their attention on botnets in their fight against criminal online activities. For this reason this session explored the different motivators behind the botnet economy and elaborate on possible steps that countries can take to take down these botnets.

[56] http://www.itu.int/ITU-D/cyb/events/2008/brisbane/docs/gercke-economics-of-cybercrime-brisbane-july-08.pdf

10. Bruce Matthews, Manager, Anti-Spam Section, Australian Communications and Media Authority (ACMA), Australian Internet Security Initiative (AISI), Australia, provided a presentation on "Australia's Spam and Zombie Botnet Initiatives: Economic Drivers"[57]. Australian internet usage is increasingly ubiquitous with an estimated 13.2 million Australians aged 14 years and over estimated to have used the internet, and in terms of media consumption Australians spend more time online than watching television. Mr. Matthews provided an insight into some spam, botnets and cybersecurity-related trends, noting that spam is the vector for substantial numbers of compromised computers and more than 90 per cent of worldwide spam is sent from botnets (with the vast majority 'criminal' spam). Overall, worldwide spam is still continuing to increase. Given that the issues seen with regards to botnets and spam are closely interrelated, addressing bots and botnets will consequently also reduce spam and enhance cybersecurity, Mr. Matthews pointed out. In this regard Mr. Matthews provided an overview of Australian integrated five part strategy to combat spam. This strategy includes: strong enforcement of the Australian Spam Act; targeted education and awareness activities; industry measures; technological initiatives and solutions; and international cooperation. He noted that a similar integrated approach is required to combat botnets.

11. Mr. Matthews also described one of ACMA key initiatives in this regards, namely the Australian Internet Security Initiative (AISI), a cooperative arrangement with Australian ISPs to shut down infected computers, and shared insights into how ISPs are using the AISI data that is provided to them on a daily basis. A pilot of AISI commenced in November 2005 with six ISPs involved and funding for enhancement and further expansion of AISI was provided by the Australian Government in 2007. AISI collects information on compromised computers, compares the IP addresses of these computers to a list of IP address ranges of Australian ISPs, and advises relevant ISP of the IP address so that the ISP can inform and liaise with the customer to fix the problem. In most cases to date, customers are completely unaware that their computers had been compromised. Currently there are 38 ISPs participating and the initiative is growing. AISI part of e-Security National Agenda "Securing Australia's Online Environment (ESNA)" and is also closely linked to DBCDE initiatives aiming at enhancing the protection of home users and small to medium to enterprises. Mr. Matthews mentioned that a number of Government agencies are now also involved in AISI's activities. Mr. Matthews also mentioned that Australia is pleased to be supporting work done in relation to ITU's Botnet Mitigation Toolkit.

12. Suresh Ramasubramanian, Consultant, India, in his presentation on the "ITU Botnet Mitigation Toolkit and Pilot Field Projects"[58] shared information on an ongoing project to develop a Botnet Mitigation Toolkit[59] to help deal with the growing problem of botnets. The *ITU Botnet Mitigation Toolkit* is a multi-stakeholder, multi-pronged approach to tracking botnets and mitigating their impact, with a particular emphasis on the problems specific to emerging internet economies. The toolkit draws on existing resources, identifies relevant local and international stakeholders and takes into account the specific constraints of developing economies. The toolkit seeks to raise awareness among Member States of the growing threats posed by botnets and their linkages with criminal activities and incorporates the policy, technical and social aspects of mitigating the impact of botnets. The first draft of the background material for the project was made available in December 2007 with pilot tests planned in a number of ITU Member States in 2008 and 2009. As part of this activity countries in the region are welcome to contact ITU-D if they have an interest in initiating a botnet mitigation pilot project in their respective countries.

Seminar Session 3: Elaboration and Development of Indicators for Cybersecurity

13. To gain an insight into the reliability of today's ICT networks and the challenges they face (and ultimately whether any progress is being made in building confidence and security in the use of ICTs), one important requirement would be to benchmark different elements of cybersecurity (e.g. spam, viruses, phishing). This benchmarking can then be used for a more detailed analysis of cybersecurity trends, both at the level of geography (national, regional, and international) and in terms of the different threats. This session looked at some of the requirements behind and usefulness of a common set of metrics for cybersecurity.

14. Hwang Seong Weon, Senior Researcher, Strategic Planning Team, Korea Information Security Agency (KISA), Republic of Korea in her presentation on the "Development of a National Information Security Index"[60] looked at the benefits of being able to measure national security through a national information security index. She started her presentation by putting an index for cybersecurity into the context of existing metrics, mentioning that the United Nations, OECD, ITU and other international organizations already collect information for different information society-related indexes and that these are used to differing degrees to establish and evaluate countries' information policies internally and externally. Ms. Weon said that the there is a need to develop an Information Security Index to analyze the current level of the internet security, to support the government to develop national IT security policies, and also fill the gap in generally accepted measuring

[57] http://www.itu.int/ITU-D/cyb/events/2008/brisbane/docs/matthews-aisi-initiatives-australia-brisbane-july-08.pdf

[58] http://www.itu.int/ITU-D/cyb/events/2008/brisbane/docs/ramasubramanian-itu-botnet-toolkit-and-pilot-brisbane-july-08.pdf

[59] http://www.itu.int/ITU-D/cyb/cybersecurity/projects/botnet.html

[60] http://www.itu.int/ITU-D/cyb/events/2008/brisbane/docs/weon-national-information-security-index-brisbane-july-08.pdf

standards in this area. She provided an insight into some of the limitations to the development of a National Information Security Index. First, it is difficult to ensure the establishment of a unified concept for information security. Second, it is difficult to select the appropriate components that accurately represent information security. Third, there is a lack of statistical data, and the reliability of surveyed statistical data is poor. The future use of a National Information Security Index would ideally indicate the characteristics of a particular group's information security. A reliable index could be used when assessing a country's information security policies together with various statistical data.

15. Karl Hanmore, Operations Manager, AusCERT, Australia in his presentation[61] and overview highlighted that while we are waiting for some useful cybersecurity metrics we still need to go on building cybersecurity capacity in all the different areas, ranging from the establishment of incident response capabilities to awareness raising campaigns. The anti-virus community is already looking into metrics and benchmarks and the data is widely shared through a number of different reports and publications, he noted. Mr. Hanmore continued by pointing out that even though the anti-virus community is relatively small, they still cannot agree on a standard set of metrics. Commercial companies and national CERTs/CSIRTs have trend reports which they share with their specific communities and constituencies.

16. There are still different views on what spam is and as consequence different numbers showing the magnitude of the spam problem. Mr. Hanmore also brought up the issue of what constitutes reliable data, and who should be collecting this data. Currently not all governments can do this on the government level, and in some instance the issue of bias for or against showing certain trends might also come into play. While some say that when it comes to metrics and number that "you cannot manage what you cannot measure", in some cases perhaps it is the numbers that drive specific outcomes. While metrics are important for funding sources, etc. the global community cannot afford to wait for metrics to do something about the overall cybersecurity threats. As immediate steps forward, Mr. Hanmore, mentioned the need to: a) Ensure constructive action now through national CERTs/CSIRTs and law enforcement. Law enforcement activities alone will not solve the problem but might reduce it. b) Strengthen relationships with the commercial sector as they hold a lot of the data that is needed. c) Gather useful metrics to support ongoing operations and combat the growing problem of online crime.

Seminar Conclusions and Recommendations.

17. The final session of the special seminar on the economics of cybersecurity discussed and reported on some of the main findings from the seminar. Mr. Saxena noted the difficulty in coming with simple solutions to complex problems but highlighted the urgency of the matter and the need to ensure that we are moving forward in building confidence and security in the use of ICTs. From the presentations and discussions during the seminar sessions, a set of recommendations emerged.

18. The seminar discussed the important aspects of the Economics of Cybersecurity, especially from the angle of the telecom operators and the overall aspect of the costs involved. It was pointed out by the Chairman that the issue involves collaboration between all stakeholders, operators as well as law enforcement agencies to ensure a collective global effort with the objective of ensuring a free and fair flow of information and communication. The members greatly appreciated the efforts made by the ITU and especially the BDT in bringing to focus the issues related to the economics of security which are gaining in importance.

19. The seminar participants expressed their appreciation for the presentations provided by the experts. They noted with particular interest the Australian Internet Security Initiative (AISA) and activities undertaken by the Australian Government in this regard, especially the involvement of the 36 ISPs that have joined forces with the government in order to shut down infected computers and inform customers about the threats associated with spam and botnets. Seminar participants felt that this model could also be utilized by other administrations in the region. The ITU Botnet Mitigation Toolkit was also seen as a good set of guidelines for countries to start considering these issues, and a useful approach to tracking botnets and mitigating their impact.

20. The seminar participants furthermore noted the need for further study into the elaboration and development of indicators to measure cybersecurity readiness. While more research and study is definitely needed in this area, the importance of reliable cybersecurity metrics at the national, regional, and international levels was highlighted by the participants as a means to attract investment as well as to facilitate global security standardization. The TAS members agreed that developing counties, which are in the process of building their networks, and members with smaller networks like those in the Pacific Island States, which have burgeoning cost of operation, require special attention and support in tackling cybersecurity-related challenges. The seminar participants felt that the complex issue of cybersecurity may require further efforts from a number of specialized multilateral agencies, especially with regards to the areas of legislation and law enforcement.

21. The seminar participants and TAS group members appreciated the effort made by ITU Development Bureau in organizing the seminar on this unique and emerging subject which is of high importance for the telecom administrations around the world, especially to the countries in the Asia-Pacific region where due to rapid growth and market pressures tariffs are declining and the costs are increasing. TAS group members encouraged continued study into the Economics of Cybersecurity by the ITU.

[61] No slides available.