International Telecommunication Union

ictQATAR
المجلس الأعلى للاتصالات وتكنولوجيا المعلومات
Supreme Council of Information & Communication Technology

ITU Regional Cybersecurity Forum 2008
Doha, Qatar

Document RWD/2008/01-E
21 February 2008
Original: English

Draft Meeting Report :

ITU Regional Workshop on Frameworks for Cybersecurity and Critical Information Infrastructure Protection (CIIP) & Cybersecurity Forensics Workshop, Doha, Qatar, 18-21 February 2008[1]

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

Purpose of this Report

1. The ITU Regional Workshop on Frameworks for Cybersecurity and Critical Information Infrastructure Protection (CIIP), and the related Cybersecurity Forensics Workshop, was held in Doha, Qatar, 18-21 February 2008. The workshop, which was hosted by ictQATAR and organized in collaboration with the Q-CERT, 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 workshop, 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 effort, including: 1) Developing a national cybersecurity strategy; 2) Establishing national government – industry collaboration; 3) Creating a national incident management capability; 4) Deterring cybercrime; and 5) Promoting a national culture of cybersecurity. The workshop also considered initiatives on the regional and international level to increase cooperation and coordination amongst the different stakeholders.

3. Approximately 100 people participated in the event, from the Arab States as well as from other parts of the world. Full documentation of the workshop, including the final agenda and all presentations made, is available on the event website at www.itu.int/itu-d/cyb/events/2008/doha/. This meeting report summarizes the discussions throughout the three days of the ITU Regional Workshop on Frameworks for Cybersecurity and CIIP, provides a high-level overview of the sessions and speaker presentations, and presents some of the common understandings and positions reached at the event. Annex 1 at the end of the document includes the shared understandings that the meeting participants agreed upon, including the Doha Declaration on Cybersecurity.[2]

ITU Regional Workshop on Frameworks for Cybersecurity and Critical Information Infrastructure Protection (CIIP) held in Doha, Qatar, 18-20 February 2008

4. 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

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

[2] The Doha Declaration on Cybersecurity can also be found online: http://www.itu.int/ITU-D/cyb/events/2008/doha/docs/doha-regional-cybersecurity-forum-output-20-feb-08.pdf

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.

Meeting Opening and Welcome

5. The Regional Workshop on Frameworks for Cybersecurity and Critical Information Infrastructure Protection was opened with a welcoming address[3] by Dr. Hessa Al Jaber, Secretary General, ictQATAR. On behalf of ictQATAR, Dr. Al Jaber welcomed the workshop participants to the event and highlighted why this workshop is an important step towards building cybersecurity capacity in the region. Dr. Al Jaber welcomed Sami Al Basheer Al Morshid, director of the ITU Development Sector (ITU-D), and Rich Pethia, founder and director of the original Computer Emergency Response Team (CERT) at Carnegie Mellon University in the United States of America. She continued by noting that for nearly twenty years CERT has been helping protect valuable information and infrastructure in countries throughout the world and, as of last year, Qatar is one of these countries. In 2007 Qatar launched a national information security program that aims to help to keep both adults and children safe on the Internet. Dr. Al Jaber noted that this initiative will also help safeguard data belonging to companies and organizations.

6. Dr. Al Jaber noted that the 2006 World Telecommunication Development Conference (WTDC-06) held in Doha, Qatar, established what has become known as the Doha Action Plan[4]. Qatar is currently moving ahead with the recommendations of the Action Plan and Dr. Al Jaber noted that since the conference, Qatar has opened its telecom market to competition and private sector participation, building common infrastructure platforms, and planting the seeds for building a truly global information society that will connect all those who live and work in Qatar to technology. The 2006 WTDC conference also sparked the formal creation of ITU-D Study Group Question 22/1, on *Securing Information and Communication Networks: Best Practices for Developing a Culture of Cybersecurity*. As the issue of cybersecurity is of pressing urgency to every nation, Dr. Al Jaber further highlighted the need to improve cybersecurity while advancing ICTs, with all of its enormous benefits. Dr. Al Jaber concluded her remarks by wishing the participants the best of luck in their work at the Regional Cybersecurity Forum, and noted that she was looking forward with great interest to the recommendations from the meeting.

7. The Director of the ITU Telecommunication Development Sector (ITU-D), Sami Al Basheer Al Morshid, followed with some opening remarks (English)[5] (Arabic)[6] on behalf of the ITU. Mr. Al Basheer said that he 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, and noted furthermore that the list of speakers and participants is very impressive and thus was sure this event will be beneficial to everyone and contribute to a deeper understanding of this very interesting subject. Mr. Al Basheer 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 weeks ago when millions of users in this region were impacted by cuts in undersea optical cables - said to be caused by an adrift boat anchor. As a result, Mr. Al Basheer continued, access to the Internet, voice calls, corporate data and video traffic were all impacted. It has been said that experience is the hardest teacher because it gives the test first and the lesson afterwards. Whatever the cause, the lesson we take away is that every nation needs to organize itself to take coordinated action related to the prevention of, preparation for, response to, and recovery from cyber incidents.

8. As cybersecurity-related goals and tasks ahead of nations are huge in importance and resources are limited, Mr. Al Basheer 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 here in Qatar and approved at our Plenipotentiary Conference in Turkey in 2006. Mr. Al Basheer noted that we are 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. Mr. Al Basheer thanked the Government of

[3] http://www.ict.gov.qa/files/DrHessaopeningremarks4%20ITUforum.pdf

[4] http://www.itu.int/ITU-D/conferences/wtdc/2006/index.html

[5] http://www.itu.int/ITU-D/cyb/events/2008/doha/docs/opening-remarks-itu-al-basheer-feb-08-english.pdf (in English)

[6] http://www.itu.int/ITU-D/cyb/events/2008/doha/docs/opening-remarks-itu-al-basheer-feb-08-arabic.pdf (in Arabic)

Qatar represented by Dr. Hessa Al Jaber, and all her team at ictQATAR and Q-CERT, for their efforts and generous hospitality, and wished the participants and organizers a successful event.

9. These opening remarks were followed by a keynote presentation on "*The Changing Cybersecurity Threat Environment*", given by Ian Cook, Team Cymru, United Kingdom. Mr. Cook's presentation looked at the evolution of cyber threats and the implications of these threats for the future. After outlining how both technology and threats have changed, with the range of threats and vulnerabilities shifting and changing through the years along with the ever-changing security landscape itself, Mr. Cook explained how the infrastructure is increasingly exposed to criminal miscreants; reviewed the open arrogance that buyers, sellers, traders, and cashiers exhibit; activities and alliances in which the underground economy is involved in; the method by which ill-gotten goods are obtained; the manner in which they advertise their services; and the personal data that is harvested every single hour of every day of the year. Mr. Cook further noted that over the past two decades, the Internet has transformed many aspects of modern life, especially the way we do business. The Internet continues to grow at a phenomenal rate and as of December 2007, he said, and an estimated one out of every five people in the world has used the Internet.

10. The Internet has enabled isolated data centers, personal computers, hand-held devices and mobile phones to transition to an environment with no perimeters and little effective protection. This has resulted in users experiencing radically different cybersecurity threats, both in nature, scope and impact from those seen only a decade ago. Mr. Cook noted that it should therefore come as no surprise, that as businesses and financial transactions increasingly use the Internet as a delivery mechanism, so has crime. Mr. Cook also described how the criminal organizations behind the implementation of these new online threats are more organized than ever before. These organizations employ software developers, buy and sell infrastructure for their criminal activities and recruit people for money laundering to hide their identities. While the Internet supports a mature and thriving underground criminal economy, Mr. Cook concluded, too little is still yet publicly known about this underground economy and how it actually works.

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

11. 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 Rich Pethia, Director, CERT Coordination Center (CERT/CC), United States of America, discussed the concept of a national framework for cybersecurity and CIIP and 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. Pethia in his opening remarks for the session highlighted the need to better try to understand the issues related to cybersecurity that have emerged due to the growing and changing use of technology, growing and changing attacks, and more technically advanced attacks. Mr. Pethia noted that the purpose of this workshop is to help countries better understand the dependencies and interdependencies that interconnection creates, and assist countries in developing national frameworks for cybersecurity.

12. Robert Shaw, ICT Applications and Cybersecurity Division, ITU Telecommunication Development Sector (ITU-D), sought to review, from a broad perspective, different approaches to cybersecurity and CIIP frameworks and their often similar components in order to provide the participants with an insight into the issues and challenges involved. Mr. Shaw provided an overview of "ITU-D Activities Related to Cybersecurity and Critical Information Infrastructure Protection"[7] and shared details on the ITU-D Cybersecurity Work Programme to Assist Developing Countries (2007-2009)[8], 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 workshops for awareness-raising and capacity building on frameworks for cybersecurity and CIIP.*

13. Mr. Shaw also shared information on an ongoing project to develop a *Botnet Mitigation Toolkit*[9] to help deal with the growing problem of botnets. The *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

[7] http://www.itu.int/ITU-D/cyb/events/2008/doha/docs/shaw-itu-d-cybersecurity-overview-doha-feb-08.pdf

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

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

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. 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.

14. Mr. Shaw furthermore 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. He noted that 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* scopes out how ITU plans to assist countries in developing cybersecurity/CIIP capacity, through, *inter alia*, 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. Mr. Shaw mentioned that one challenge in moving forward on discussions relating to cybersecurity was finding appropriate mechanisms for the different actors to better communicate with each other, given that each group of actors often have different and specific requirements as to the levels of trust needed to share specific information. Mr. Shaw also mentioned that the ITU hopes to launch a Cybersecurity Fellowship Programme[10] later this year.

15. James Ennis, Department of State, United States of America, in his capacity as the Rapporteur for ITU-D Study Group 1 Question 22 — *Securing Information and Communication Networks: Best Practices for Developing a Culture of Cybersecurity*, followed 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. In his presentation "Best Practices for Organizing National Cybersecurity Efforts"[11], he explained the background of work in the Study Group and particularly its report on *Best Practices for Organizing National Cybersecurity Efforts*[12], which governments can use as a guideline when developing and undertaking national strategies for cybersecurity and CIIP. Mr. Ennis invited workshop participants and country representatives to join the Q22/1 activities, which were initiated at the 2006 World Telecommunication Development Conference (WTDC-06). Three Study Group Q22/1 meetings have taken place to date, with the next meeting scheduled for 21-22 April 2008.

16. The report being developed by the Study Group addresses the major problems that policy makers are faced with when dealing with cybersecurity. The draft report starts with a working definition of cybersecurity ("Cybersecurity is the prevention of damage to, unauthorized use of, exploitation of, and - if needed - the restoration of electronic information and communication systems, and the information they contain, in order to strengthen the confidentiality, integrity and availability of these systems."), and notes that different levels of security are necessary for different systems, and highlights the need for adequate risk management. 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) National Incident Management Capabilities; and, 5) A National Culture of Cybersecurity, noting also that national cybersecurity awareness has an international component.

17. The draft report 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 specific step. Mr. Ennis 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. However, he also mentioned that the report is only as good as the contributions that countries feed into the report and the work of the Study Group, and with this asked countries present at the meeting to share their best practices that could be of use to the other countries in developing a framework for national cybersecurity efforts. In conclusion, Mr. Ennis recognized that presently all critical sectors of society rely on information and communication networks for their stable functioning, and in order to achieve a maximum level of security, these systems need to be reliable, secure, and trusted. All nations, including both developed and developing countries, are affected by this.

Session 2: Management Framework for Organizing National Cybersecurity/CIIP Efforts

18. 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

[10] http://www.itu.int/ITU-D/cyb/cybersecurity/

[11] http://www.itu.int/ITU-D/cyb/events/2008/doha/docs/ennis-cybersecurity-best-practices-doha-feb-08.pdf

[12] 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

involved? Are there examples of frameworks that can be adopted? Sessions 2 and 3 sought to explore in more detail various approaches, best practices, and identify key building blocks that could assist countries in establishing national strategies for cybersecurity and CIIP. Specifically, the two sessions presented in further detail the *ITU Framework for Organizing a National Approach to Cybersecurity* and its five key elements of national cybersecurity effort, including 1) Developing a national cybersecurity strategy; 2) Establishing national government – industry collaboration; 3) Deterring cybercrime 4) Creating national incident management capabilities; and 5) Promoting a national culture of cybersecurity. In order to share more information on the structure of the Framework and provide meeting participants with ideas on how the Framework might work for countries in the region, the first of the two sessions, moderated by Bradford Willke, Senior Technical Staff, Survivable Enterprise Management, CERT, Carnegie Mellon University, United States of America, looked closer at the components dedicated to: Promoting a Culture of Cybersecurity; Government – Industry Collaboration; and Incident Management Capabilities.

19. Christine Sund, Cybersecurity Coordinator, ICT Applications and Cybersecurity Division, ITU Telecommunication Development Sector (ITU-D), in her presentation on "Promoting a Culture of Cybersecurity"[13] provided an overview of what a culture of cybersecurity means and what could be 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)[14] 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.

20. 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 noting though at the same time that cybersecurity at its core is a shared responsibility.

21. Bradford Willke, Senior Technical Staff, Survivable Enterprise Management, CERT, Carnegie Mellon University, United States of America, continued with his presentation on "Government – Industry Collaboration"[15]. Mr. Willke started by providing an introduction to the concept of government – industry collaboration, noting that the main goal involves establishing collaborative relationships to manage cyber-risk and to better protect cyberspace. These relationships provide a mechanism to bring government and industry perspectives, equities, and knowledge together in order to reach consensus and move forward to enhance security at the national level. Mr. Willke highlighted the importance of actively working to reduce possible barriers to government – industry collaboration by focusing on mechanisms to build trust and promote collaboration, through, among other things; utilizing a written agreement that guides the collaboration and exchange between government and industry, defining a shared vision and purpose, and leveraging strong individual and organizational leadership to enable the participants to achieve tangible and measurable outcomes.

22. In conclusion Mr. Willke provided an insight into four case studies of government – industry collaboration, all with specific lessons learned. These included the following initiatives: 1) The Malaysian Information Sharing Forum (ISF), which is a forum for Internet Service Providers (ISPs) and government agencies to address Malaysian information and network security issues. 2) The Financial Information Security Alliance in the Republic of Korea, which aims to protect financial information security systems from cyber-terror and hacking through the development of information protection standards and policies for the financial sector as well as assessments and certifications, among other things, and the Information Security Practice Alliance which is a voluntary alliance of private and public sector organizations which aim to increase information protection activities in the private sector, in cooperation with various security companies and associations and with the help of the Korean

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

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

[15] http://www.itu.int/ITU-D/cyb/events/2008/doha/docs/willke-government-industry-collaboration-doha-feb-08.pdf

Information Security Alliance (KISA). 3) The Critical Infrastructure Protection Modeling and Analysis (CIPMA) Program in Australia, which seeks to enhance the protection of Australia's critical infrastructure and improve the resilience of the economy and society as well as build technology for modeling and analyzing relationships and dependencies between Australia's critical infrastructure systems. The initiative also aims to build a capability to model and report on the likely impacts when networks in one or more sectors are affected by failures (caused by nature or people) in another sector. Sectors covered to date include energy, telecommunications, and banking and finance. 4) The National Infocomm Competency Centre (NICC) in Singapore, which is an industry-led and government-supported organization created to assist individuals and organizations in reaching and maintaining a high level of ICT competence. Working closely with the Ministry of Manpower (MOM) and the Infocomm Development Authority (IDA) it aims to promote knowledge and skills, and also serves as the main accreditation body for ICT certifications.

23. This presentation was followed by Ian Dowdeswell, Manager, Watch, Warning, Investigation, and Response, Q-CERT, Qatar, with a presentation on "Incident Management Capabilities"[16], providing an overview of Q-CERT structure and activities and how these link directly in with the ITU Cybersecurity Framework pillar "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. Dowdeswell noted, 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.

24. Mr. Dowdeswell 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. Dowdeswell 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.

25. In the evening of the first day of the workshop the participants were invited by the organizers to a reception at the workshop venue, the Doha Marriot Hotel.

Session 3: Management Framework for Organizing National Cybersecurity/CIIP Efforts (Continued)

26. Session 3 of the meeting continued to look closer at the remaining components of the *ITU Framework for Organizing a National Approach to Cybersecurity*, namely Deterring Cybercrime and a National Cybersecurity Strategy. The Session 3 moderator, Sherif Hashem, Ministry of Communications and Information Technology, Egypt introduced the speakers in the session, and highlighted the growing problems related to different legal frameworks in countries around the world and the urgent need for increased collaboration between all countries in this area.

27. Nibal Idlebi, ICT for Development Team Leader, Information and Communication Technology Division, United Nations Economic and Social Commission for West Asia (UN-ESCWA), opened the session with her presentation on "Legal Foundation and Enforcement: Cyber Legislation in the ESCWA Region – Security Issues"[17]. Ms. Idlebi noted that active efforts are essential for the establishment of the enabling environment that is needed for effective and ethical use of cyberspace, and cyber-legislation is a key enabling component in the development of a modern information society. Furthermore, with regards to cyber-related legislation in the ESCWA region, regional integration is important for improving the electronic transaction between countries in the region. Ms. Idlebi provided an overview of a UN-ESCWA survey of international and regional and national legislation for data protection and privacy, and the status in the ESCWA region in this regard.

28. Ms. Idlebi noted that many countries have not yet enacted laws to prevent computer crimes. Examples of initiatives from the region were shared with the meeting participants, this included the United Arab Emirates' Federal Law No. 2 of 2006 on Combating Information Technology Crimes, the Law on Electronic Crime passed in Saudi Arabia in 2006, and the activities taking place in the Gulf States, notably with Bahrain and Qatar drafting cybercrime legislation which they hope will be enacted soon. Other ESCWA Member States, Ms. Idlebi noted, currently rely on the provisions in existing penal codes, copyright laws and to the extent in which these extend to cybercrimes. Overall, however, she said, there is a real lack of legislation to criminalize the misuse of ICTs in

[16] http://www.itu.int/ITU-D/cyb/events/2008/doha/docs/dowdeswell-incident-management-qcert-doha-feb-08.pdf

[17] http://www.itu.int/ITU-D/cyb/events/2008/doha/docs/idlebi-cyber-legislation-ESCWA-doha-feb-08.pdf

the region. Therefore, the UN-ESCWA study recommends its 13 Member States in the region to address the lack of cyber-related legislation either by ratifying relevant international conventions or enacting national laws that are compliant with international agreements and/or national laws. This can be undertaken through the creation of a specialized focus group for the drafting of cyber legislation, together with interviews, workshop and discussions of draft legislation with the concerned parties. Ms. Idlebi concluded her presentation by providing an insight into the UN-ESCWA Template for Cyber Legislation Development, which aims to assist Member States in formulating cyber-related legislation. Ms. Idlebi showed a live demo of the soon to be UN-ESCWA launched website that has been developed to support these activities.

29. Building on the presentations made earlier in Sessions 1 and 2 of the workshop that showcased the different pillars of the framework for cybersecurity and CIIP and different national strategies and approaches, Joseph Richardson, United States of America, with his presentation on "A National Cybersecurity Strategy"[18], described the final element of the Framework which ties the other components together, namely the development of a national cybersecurity strategy. Emphasizing that the protection of cyberspace is essential to national security and economic well-being, Mr. Richardson provided some concrete ideas how countries can get started on developing a national strategy. An important tool in this effort is the ongoing ITU work to develop a comprehensive National Cybersecurity/CIIP Self-Assessment Toolkit[19]. Representing one of the key synergies between ITU-D Study Group Q22/1 work on "Securing information and communication networks: Best practices for developing a culture of cybersecurity"[20] and the ITU Cybersecurity Work Programme to Assist Developing Countries (2007-2009)[21] activities, the ITU National Cybersecurity/CIIP Self-Assessment Toolkit applies the framework under development in the Study Group with a practical toolkit for consideration at the national level.

30. 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 that was presented by Mr. Ennis in Session 1. 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.

Session 4: Country Case Studies

31. In order to further explore how different countries are currently implementing the five pillars of the Management Framework for Organizing National Cybersecurity/CIIP Efforts, i.e., Promoting a Culture of Cybersecurity, Government — Industry Collaboration, Incident Management Capabilities, Legal Foundation and Enforcement, and A National Cybersecurity Strategy, Sessions 4, 5, and 6 were dedicated to specific country case studies. Session 4, moderated by Marilyn Cade, Advisor to AT&T, United States of America, looked closer at case studies relating to Promoting a Culture of Cybersecurity and Government — Industry Collaboration.

32. The first country case study on promoting a culture of cybersecurity, was presented by Raja Azrina Raja Othman, Chief Technology Officer, CyberSecurity Malaysia, Malaysia, "Promoting a Culture of Cybersecurity Among Critical National Information Infrastructure"[22]. The Malaysian National Cyber Security Policy (NCSP) was initiated by the Ministry of Science, Technology and Innovation in 2006, to harness national effort to enhance the security of Malaysia's Critical National Information Infrastructure (CNII). The NCSP is structured around eight main cybersecurity policy thrusts, similar to the five pillars of the ITU Cybersecurity Framework but where some of these pillars have been broken up further to meet specific Malaysian requirements. Ms. Raja Othman mentioned that the 4th policy thrust is dedicated to a culture of security and 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 CNII. Establishing an effective mechanism for cybersecurity knowledge dissemination at the national level and identifying minimum requirements and qualifications for information security professionals is also an important part of this activity. Furthermore, Ms. Raja Othman mentioned ethics as a key component of the Cybersecurity Malaysia programme.

33. Ms. Raja Othman shared examples of different Malaysian initiatives with the meeting participants, including the Knowledge Sharing Platform that have been launched to increase cybersecurity awareness at the national

[18] http://www.itu.int/ITU-D/cyb/events/2008/doha/docs/richardson-cybersecurity-framework-and-readiness-assessment-doha-feb-08.pdf

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

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

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

[22] http://www.itu.int/ITU-D/cyb/events/2008/doha/docs/othman-promoting-a-culture-of-cybersecurity-malaysia-doha-feb-08.pdf

level. She mentioned that cybersecurity and Internet safety awareness campaigns and related outreach programs had started with identifying the partners that needed to be involved, following this a lot of awareness-raising material, such as specific content, portals, websites, etc., had been developed to meet the needs amongst the Malaysian population, and more importantly tailoring this information to specific target audiences.[23]

34. Getting the information across to the intended audience has proven a challenge. Ms. Raja Othman mentioned that the Cybersecurity Malaysia team has been working closely with the Ministry of Education to reach students and teachers, the Ministry of Information to make information available through radio channels, and other means, in order to focus the limited resources available on content development and seek to partner with others to reach out and make the material more widely available to the citizens. Ms. Raja Othman also described the Competency Development Programs which includes information security certifications, and the Critical National Information Infrastructure (CNII) Portal, which is a security resource portal designed specifically to meet the needs of security practitioners (management and technical) within CNII organizations. In conclusion, to promote a national culture of cybersecurity, Ms. Raja Othman re-emphasized the need to innovate and generate material relevant to specific the target audiences and to expand partnerships with key stakeholders in order to better reach out to the end users. Assessing the effectiveness of initiatives undertaken, through surveys and other mechanisms, was also highlighted as necessary step moving forward.

35. Laile Di Silvestro, Business Operations Manager, Microsoft Corporation, followed with a presentation on "Government – Industry Collaboration: 7 Steps for Resiliency in Critical Infrastructure Protection"[24]. Ms. Di Silvestro emphasized that in order to realize the vast promise of information technology, partnerships between the public sector and private sector actors in the interests of security are essential. Increased cybersecurity can only be achieved through government and industry working together. Such partnerships are necessary in all aspects of the critical infrastructure protection framework, to effectively assess risk, mitigate threats, detect exploits and attacks, and respond rapidly in the event of an attack. The purpose of the 7 Resiliency Steps approach presented is to provide a set of elements of best practices from different regions in the world that governments have adopted. With these guiding principles in mind, government, infrastructure owners and operators can collaboratively pursue a set of core enablers of resiliency and infrastructure.

36. The 7 Steps include: 1) *Define goals and roles*. Establishing clear goals is central to generate support for cybersecurity by the different stakeholder groups while better understanding the different roles of the stakeholders promotes coordination, efficiency and trust. 2) *Create public-private partnerships*. Ms. Di Silvestro explained that the creation of trusted relationships is critical to information sharing and developing solutions to difficult problems. Leveraging the unique skills of government and private sector organizations are necessary to address today's dynamic threat environment. 3) *Identify and prioritize critical functions*. Close collaboration is needed to understand the interdependencies involved. 4) *Continuously assess and manage risks*. Assessing risk, identifying controls and mitigations, implementing controls and measuring effectiveness are important aspects of continuous risk management. 5) *Establish and exercise emergency plans and improve operational coordination*. Emergency response plans can mitigate damage and promote resiliency. 6) *Build security and resiliency into operations as security is a continuous process*. Leveraging security principles promotes secure and resilient organizations. 7) *Update and innovate technology and processes*. While cyber-threats are constantly evolving policy makers, enterprise owners, infrastructure operators can still prepare for and mitigate these threats by keeping the technologies they are using current and up-to-date.

37. In conclusion Ms. Di Silvestro shared details on some of the cybersecurity initiatives which Microsoft has launched, including the Microsoft Security Cooperation Program, a worldwide program for governments and governmental organizations responsible for computer incident response, protection of critical infrastructure, and computing safety to collaborate in the area of IT security. Ms. Di Silvestro noted that many countries in the region are already involved in this initiative.

38. Marilyn Cade, Advisor to AT&T, United States of America, in her presentation "Country Case Studies for Government - Industry Collaboration"[25], discussed some of issues that need to be addressed when it comes to government – industry collaboration for cybersecurity. Ms. Cade noted that the users on the Internet are changing but so is the traffic on the Internet. While everyone is annoyed by spam clogging up e-mail boxes, the volume of the traffic on the Internet is currently made up mostly of peer-to-peer (P2P) and file sharing. What providers need are responsible and ethical Internet users. However, when customers become too costly to support then the private sector will act and start looking into possible solutions. Governments are considering the same problems. Ms. Cade drew the meeting participants' attention to the fact that the majority of the content on the Internet is still mainly in English. However, in order to be able to best promote a global culture

[23] http://www.esecurity.org.my/

[24] http://www.itu.int/ITU-D/cyb/events/2008/doha/docs/di-silvestro-government-industry-collaboration-casestudies-doha-feb-08.pdf

[25] http://www.itu.int/ITU-D/cyb/events/2008/doha/docs/cade-government-industry-collaboration-casestudy-doha-feb-08.pdf

of cybersecurity, cybersecurity awareness-raising resources and material need to be made available in local languages.

39. Ms. Cade showed some examples of awareness-raising initiatives from around the world that have been developed from government collaboration with industry. She noted that there is a need for both a "pull" and a "push" approach when it comes to cybersecurity outreach, ensuring that a lot of information is available online proving easy-to-understand instructions on how citizens can protect themselves (pull approach) and providing resources to allow for awareness-raising officers to go out in schools, work places, etc. to train users how to act responsibly when online (push approach). Ms. Cade noted that from an industry point of view an informed customer is a much better user and thus a better customer. There are many existing models and examples of how governments and industry (and not for profits) are working together to provide information on cybersecurity for businesses of all sizes, families, children, schools; organizations, including governmental agencies. There is no one solution, but industry usually offers unique skills, expertise, and information. Often discussions between government agencies and industry lead to the creation of the online service, and furthermore government interest keeps industry engaged.

Session 5: Country Case Studies (Continued)

40. In Session 5 discussions related to the different components of the ITU Cybersecurity Framework continued with examples of country case studies. This session, with Julia Allen, Member of Technical Staff, Software Engineering Institute, Carnegie Mellon University, United States of America, as the session moderator, looked closer at country case studies related to Incident Management Capabilities and the need for a Legal Foundation and Enforcement.

41. The first presentation in this session was delivered by Belhassen Zouari, Chief Executive Officer, National Agency for Computer Security and Cert-Tcc, Tunisia, Country Case Study — Incident Management Capabilities, "Watch, Warning and Incident Response Capabilities : Implementing a National Strategy"[26]. Mr. Zouari from Cert-Tcc, which is the only FIRST[27] -recognized Computer Emergence Response Team (CERT©) on the African continent and the third CERT in the Arabic-speaking countries, gave the participants an overview of how the agency came into being. At the end of 1999, a unit (a "Micro-CERT"), specialized in IT Security was created. The original objective of the unit was to raise awareness amongst decision makers and technical staff about security issues and to create the first taskforce of Tunisian experts in IT Security with the goal of monitoring the security of highly critical national infrastructures and applications. In 2002, the unit started to establish a strategy and a National Plan in IT Security.

42. In January 2003, there was a decision of the Council of Ministers, and headed by the President, to create a national agency specialized in IT security in order to facilitate the execution of the national strategy. As a result, in September 2005, the Computer Emergency Response Team – Tunisian Coordination Center (Cert-Tcc) was launched. Some of the activities that Cert-Tcc is involved in include; watch, warning, and information dissemination, awareness (involving different kinds of awareness-raising campaigns, developing a culture of cybersecurity, information for judges, etc.), information sharing, analysis and collection, incident handling, coordination, etc. Cert-Tcc also provides specific expertise on IT security. The partners that Cert-Tcc engages with differ depending on the activity in question. Mr. Zouari noted that ISPs are an important partner in this activity as they manage ports that go in and out of the country. Mr. Zouari also emphasized what had already been mentioned by speakers before him — that while all cybersecurity awareness-raising initiatives are undertaken with the overall goal to promote a culture of cybersecurity, there is a clear need for specific awareness-raising material and programs depending on communities that are targeted.

43. The next speaker, Mark Krotoski, National Coordinator, Computer Hacking and Intellectual Property Program, Computer Crime & Intellectual Property Section, Department of Justice, United States of America, presented case studies related to the legal foundation and enforcement aspect of the ITU Cybersecurity Framework. Mr. Krotoski started his presentation, "Legal Foundation and Enforcement: Promoting Cybersecurity", by discussing the role in cybersecurity for legal foundation and enforcement, and how effective the criminal justice system is in countries in deterring crime, and how far global enforcement can reach in this respect. Mr. Krotoski walked the participants through different case examples demonstrating how almost every case that prosecutors deal with today, whether organized crime, gambling, kidnapping, etc., has some computer-related component. Cybercrime no longer involves only attacks on computers but also involves a large number of people who use computers in everyday life and these numbers are growing rapidly. He mentioned the need to consider the great potential for economic growth that the Internet can bring, but at the same time noting that all these benefits depend on reliable and secure information networks, and that these are in danger if a country cannot provide secure information networks for citizens and businesses.

44. A legal foundation and related enforcement are essential for effective cybersecurity as it provides a framework to investigate, prosecute and deter cybercrime, promote cybersecurity, as well as increasing confidence in legal systems and encouraging commerce. Therefore, it is increasingly important for each country

[26] http://www.itu.int/ITU-D/cyb/events/2008/doha/docs/zouari-incident-response-tunisia-doha-feb-07.pdf

[27] http://www.first.org/

to develop capabilities and competences required to investigate abuse or misuse of networks and ensure that criminals who attack or exploit the networks are punished. There are numerous challenges that the legal foundation faces, including the growing sophistication of the crimes committed online, and the increasingly organized nature of these crimes. When dealing with threats that aim to directly harm individuals, where for instance e-mail is being used but the threat is physical, evidence to solve the crime is often located abroad. Therefore, the international dimension of these cases cannot be overlooked. Noting at the same time that often there is still a lack of trust between the different organizations that need to cooperate for solving a crime. When considering the investigations associated with each crime, the ability of investigators to investigate computer related crimes, collect and preserve evidence and the time sensitivity in this, must be taken into account. Specialized training, Mr. Krotoski noted, is therefore a very important part of any national program to deter cybercrime and build enforcement capacity.

Session 6: Country Case Studies (Continued)

45. Session 6 looked closer at the different building blocks needed to develop a successful National Cybersecurity Strategy, with some examples from countries in the region. The session was chaired by Shamsul Jafni Shafie, Director, Security, Trust and Governance Department, Malaysian Communications and Multimedia Commission (MCMC), Malaysia.

46. Steve Huth, Director, Q-CERT, Qatar, in his presentation "Case Study on National Cybersecurity Strategy – Qatar"[28], provided an insight into the ongoing and planned initiatives in Qatar, through ictQATAR and Q-CERT activities, related to establishing a national cybersecurity strategy. In obtaining agreement on the development of a national cybersecurity strategy, Mr. Huth 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. In order to achieve the national vision (ictQATAR's vision) to "connect people to the technologies that will enrich their lives, drive economic development and inspire confidence in our nation's future", Q-CERT was established in 2006 to ensure among other things that the information and communication technology deployed in the country is secure and resilient. With Q-CERT activities maturing, Mr. Huth 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.

47. Mr. Huth 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 see assess where they are at in the development of their national cybersecurity efforts, and where more work is needed going forward. Mr. Huth 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. 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 go back and adjust your activities. Mr. Huth proposed that each organization sketch out what the world looks like according to their specific organization, and then compare the planned strategy to this sketch. 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. Huth 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. Huth 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 is therefore a critical component of the implementation of any national cybersecurity strategy.

48. Fatma Bazargan, aeCERT, Telecom Regulatory Authority, United Arab Emirates, in her presentation "A National Cybersecurity Strategy – aeCERT Roadmap"[29], explained the vision and role of the United Arab Emirates Computer Emergency Response Team (aeCERT), the national UAE CERT, in implementing the overall UAE plan for cybersecurity. aeCERT was established on the initiative of the UAE Telecommunications Regulatory Authority (TRA) as an advisory body which can recommend the adoption of good practice policies, procedures and technologies to detect, prevent and respond to current and future cybersecurity incidents in the UAE. Ms. Bazargan also mentioned that aeCERT actively works to promote, build and ensure a safer cyber environment and culture in the UAE. aeCERT was launched in 2007, and when fully operational, will serve the government, law enforcement and business sectors in the UAE. Ms. Bazargan highlighted the importance of an overall picture

[28] http://www.itu.int/ITU-D/cyb/events/2008/doha/docs/huth-incident-management-qcert-doha-feb-08.pdf

[29] http://www.itu.int/ITU-D/cyb/events/2008/doha/docs/bazargan-national-strategy-aeCERT-doha-feb-08.pdf

and plan before establishing and launching a CERT, like aeCERT, and emphasized the conscious decision made by aeCERT to start small and grow with time.

49. Ms. Bazargan shared information on an ongoing national security awareness campaign, which is the first of its kind in UAE. The campaign was launched in November 2007 around the theme of "protecting your online identity" and focuses on raising awareness on topics such as password security, social engineering, and more generally on the essentials of information security. Material for the campaign has been prepared in Arabic and English and targets businesses, home users and students.

50. Suliman A. Al Samhan, Information Security Specialist, SA-CERT, Communications and Information Technology Commission, Saudi Arabia, provided with his presentation an insight into the activities of the "Saudi Arabia Computer Emergency Response Team"[30], SA-CERT. Working with the vision to be the trusted authoritative reference for information security in the Kingdom of Saudi Arabia, SA-CERT through its activities and initiatives aims to improve the information security awareness level in the country. Mr. Al Samhan noted that the SA-CERT team works towards this goal through coordinating national and international efforts, by promoting IT Security best practices and creating trust amongst the cyber community, through information security capacity building, and promoting and supporting a trusted e-transactions environment, among other things.

51. Mr. Al Samhan shared information with the participants on the three phases of setting up SA-CERT and its related activities. Phase 1 included planning and the initial implementation of baseline operations through building awareness and trust, and the necessary response capabilities. Phase 2 requires incremental steps to ramp up operation capability and related capacity building, through establishing activities to monitor, response, coordinate related initiatives. Finally, Phase 3 will be full operation of all related activities. At the moment, SA-CERT is mainly focusing on cybersecurity awareness-raising with awareness programmes in Arabic, and stepping up and increasing services offered. As noted by the other speakers in the session, Mr. Al Samhan also highlighted the need to have trained and dedicated national staff and people capable of supporting the activities of the CERT. Mr. Al Samhan mentioned that they have found out that there is a dire need for a national reference center and system that provides information on cybersecurity. To meet this need an "Information Security Handbook" has been developed. The Handbook will be made available in Arabic and English on the SA-CERT website shortly. Mr. Al Samhan mentioned that the team is currently developing a lot of different cybersecurity awareness-raising material, referred to as "security handouts", in Arabic, on topics such as wireless security, email security, protecting home PCs from Internet threats, privacy, spam, phishing, as well as a parental guide promoting child safety on the Internet.

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

52. Session 7, the final session of the day, sought to review and further discuss the *Management Framework for Organizing National Cybersecurity/CIIP Efforts*, identifying some of the main takeaways from the presentations on the Framework and the related country case studies in preparation for the concluding workshop discussions. To help organize the session, the session moderator: Robert Shaw, Head, ICT Applications and Cybersecurity Division, ITU Telecommunication Development Sector (ITU-D), asked six panelists to give their main takeaways from the six sessions already held and, if possible, provide some proposals and recommendations for practical next steps in the region.

53. Marilyn Cade, Advisor to AT&T, United States of America, noted that we are still in the early days of building a culture of cybersecurity, and in the early stages of building a framework in each country. Therefore, we can start to think about the commonalities, across the different workshops that are taking place, and pull the information from these and match with our needs to continue to share information, and collect information that can be shared with other countries (e.g., approaches that work and do not, etc.). Ms. Cade noted that when talking about government – industry collaboration, we need to make sure that we continue to involve industry, and also ask who else from industry needs to be involved, at national, regional, and international levels. In the overall cybersecurity ecosystem there are so many parties that need to be involved, and due to this, Ms. Cade mentioned the need to also reach out to regional network operator groups (NOGs), Regional Internet Registries (RIRs), country code Top Level Domain (ccTLD) operators, etc., to ensure that they are invited to future workshops on this topic in order to truly be able to build a culture of cybersecurity.

54. Suliman Al Samhan, Information Security Specialist, SA-CERT, Communications and Information Technology Commission, Saudi Arabia, mentioned that the most important thing that has happened in the area of cybersecurity in Saudi Arabia and in GCC countries is the issuing of necessary laws so that people start thinking about the impact of their actions. In most cases, these laws will also start putting requirements on ISPs to keep and store information for possible future needs. Furthermore, capacity building in cybersecurity is key. Banks and telecom companies already have good security staff but more capacity building is urgently needed. Capacity building and awareness-raising, through different programs and initiatives, requires and deserves even more attention in the region.

[30] http://www.itu.int/ITU-D/cyb/events/2008/doha/docs/alsamhan-national-strategy-CERT-SA-doha-feb-08.pdf

55. Shamsul Jafni Shafie, Director, Security, Trust and Governance Department, Malaysian Communications and Multimedia Commission (MCMC), Malaysia, noted that after listening to presentations from the different CERT teams in the region, it is refreshing to hear about strategies and objectives coming from these recently established teams. The approaches presented are clearly based on the experiences that other CERT teams have learned. From a policy and enforcement point of view, Mr. Shafie continued, it is very important to have the right policies and enforcement in place when addressing cybersecurity. It is relatively easy to get information on and help with the drafting of legislation but the problem really lies on the enforcement side of this. Increasing the understanding amongst prosecutors, and all different levels of enforcement, requires extensive training. The banking regulator, the communications regulator, as well as the normal police need knowledge about cybercrime. Apart from having the right laws and enforcement, the capacity building aspects need to be addressed quickly. Having the right people at the right places to do what needs to be done is key. Mr. Shafie noted ITU-D's work in the countries and regions in creating a culture of information sharing, and hoped this can continue also in the future. Furthermore, when undertaking these efforts, we need to remember that we are not alone, as other countries are trying to address the same issues.

56. Bradford Willke, Senior Technical Staff, Survivable Enterprise Management, CERT, Carnegie Mellon University, United States of America, noted that when considering the real design and recipe for the activities involved, we should also start looking at risk capacity criteria. Mr. Willke noted that incident management is more than just about technology. The conversations that take place need to have the eye on one goal; a quantifiable measure of what you do not want to happen and also what it is that you want the economy to have. The implications of trust in government could also be one of these parameters. Spam, for example, is a culturally measurable barometer, where some things are more or less acceptable. Doing nothing about spam shows what is important to a nation. Openness of the model adopted is recommended as is the need to think nationally but plan globally. In Qatar, for example, communications infrastructures are key, therefore in achieving our goals, we need to work on establishing working government – industry collaboration in this area. There is a lot of industry collaboration already taking place, and governments needs to tap into this in order for not to disturb this collaboration with new policies.

57. Sherif Hashem, Executive Vice President, Information Technology Industry Development Agency, Ministry of Communications and Information Technology, Arab Republic of Egypt, brought the participants' attention to the roles and responsibilities connected to the ITU Cybersecurity Framework. As there are many different government agencies, and private sector stakeholders (companies, multinationals, SMEs, etc) that could be involved, we need to be clear on who we are talking about. The impact of cybersecurity touches everyone, and therefore all parties need to be involved in the process of defining and implementing a national strategy for cybersecurity. When looking at developing a national cybersecurity strategy, all stakeholders need to be involved in this effort, directly or indirectly. High level direction and buy-in is also a prerequisite. When looking at the roles and responsibilities of the different stakeholders and the collaboration between these, defining what is meant with collaboration should also be considered. The role of the ITU and other international organizations in sharing information and distributing best practices is a very important effort. Mr. Hashem also noted the importance of a technology neutral approach in countering cyber-related crimes.

58. Joseph Richardson, United States of America, as the final speaker on the panel, noted in his comments that he had heard some good reasons why governments should work with industry for cybersecurity and 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. Especially one area that needs to be further developed is the role of relationships, the relations 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 these cybersecurity workshops and related activities. Mr. Richardson concluded by noting that he had not heard anything that implies that the ITU Cybersecurity Framework is not a useful tool for building cybersecurity capacity.

Sessions 8 & 9: ITU National Cybersecurity/CIIP Self-Assessment Toolkit: An Exercise

59. The ITU National Cybersecurity/CIIP Self Assessment Toolkit[31] is based on studies underway in the ITU Telecommunication Development Sector's Study Group 1 Question 22: *Securing information and communication networks: Best practices for developing a culture of cybersecurity*. Representing one of the key synergies between the Q22/1 work and the ITU Cybersecurity Work Programme to Assist Developing Countries (2007-2009)[32] activities, the ITU National Cybersecurity/CIIP Self-Assessment Toolkit applies the framework under development in the Study Group with a practical toolkit for consideration at the national level. The toolkit is intended to assist national governments in examining their existing national policies, procedures, norms, institutions, and relationships in light of national needs to enhance cybersecurity and address critical

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

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

information infrastructure protection. The toolkit is directed to leadership at the policy and management levels of government, and addresses the policies, institutional framework, and relationships for cybersecurity. It seeks to produce a snapshot of the current state of national policy and capability, of institutions and institutional relationships, of personnel and expertise, of relationships among government entities and relationships among government, industry and other private sector entities.

60. Sessions 8 and 9 of the workshop aimed to take countries in the region through the self-assessment process to help governments understand their existing efforts, identify gaps that require attention, and prioritize national efforts and practical implications of the framework. Joseph Richardson, who acted as the facilitator for the exercise, in guiding the countries through the self-assessment, 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 a national strategy for cybersecurity and CIIP.

61. 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 workshops organized by ITU in 2008, and 2009. The moderator also further encouraged meeting participants to share country specific experiences and ask questions from the experts that had presented on each of the five pillars of the ITU Cybersecurity Framework.

Session 10: Regional and International Cooperation

62. Regional and international cooperation is extremely important in fostering a culture of security, along with the role of regional fora to facilitate interactions and exchanges. This session reviewed some of the ongoing regional and international cooperation initiatives in order to inform meeting participants about and encourage them to support and participate in further concrete actions that could be implemented in the Arab States as well as internationally. The moderator of the session, Michael Lewis, Deputy Director, Q-CERT, Qatar, opened the session and introduced the four meeting speakers.

63. Mark Krotoski, National Coordinator, Computer Hacking and Intellectual Property Program, Computer Crime & Intellectual Property Section, Department of Justice, United States of America and Representative for the 24/7 High Tech Crime Network, in his presentation on "Promoting Regional and International Cooperation On Cybersecurity Issues"[33] provided an insight into the activities of the 24/7 High Tech Crime Network. The purpose of the 24/7 High Tech Crime Network, originally a G8 initiative, is to provide an emergency contact network for online crime issues. The network is made up of law enforcement people who share information and advice related to data preservation, ISP contacts, and how to start mutual legal assistance processes. Currently the 24/7 High Tech Crime Network has contact points in close to 50 countries with, in addition to G8 members, many Asian, European, and South American countries involved. The network is open to all countries and joining the 24/7 network is quite easy and straightforward. The only requirement is availability but this does not necessarily mean a commitment to help. Countries interested in joining the network need to identify a primary contact point who has sufficient technical knowledge when it comes to dealing with cyber-related crimes — particularly as one of the main issues with cybercrime is handling digital forensic evidence. The 24/7 High Tech Crime Network contact point also needs to know something about domestic laws and procedures in this specific topic area. Mr. Krotoski mentioned that countries interested in learning more about the network can contact the US Department of Justice Computer Crime and Intellectual Property Section (CCIPS).

64. Ebrahim Al-Haddad, Head, ITU Regional Office for Arab States, gave the participants an insight into some of the current and planned activities that the ITU and the ITU Regional Office for Arab States are undertaking to further promote a culture of security in the region. Mr. Al Haddad mentioned that ITU through the WSIS process was asked to act as the facilitator for activities that fall under WSIS action line C5 dedicated to building confidence and security in the use of ICTs. However, ITU can only accomplish the tasks that was set upon it is by working with its Member States, meaning also those countries from the region that are present at this cybersecurity workshop. Building trust amongst the stakeholders is difficult and takes time, and as the ITU regional office it is our responsibility to take into account the needs of the 22 Arab countries who are members of the League of Arab States. This workshop in Doha is one in a series of ITU cybersecurity events that will take place all around the world in 2008/2009 and ITU is working closely with a number of relevant international and regional organizations to try to ensure that countries work together on cybersecurity related matters. With the growing number of regional and international cybersecurity events it is clear that one person cannot participate in all of them, therefore each country needs to select those events, workshops, and interest areas that are relevant to that country. It is clear though that we cannot work in isolation for cybersecurity, we rely on other people and need the assistance of others, regional support and collaboration is therefore increasingly important in this effort.

65. Majid Al Sharhan from Saudi Arabia, representing the Gulf Cooperation Council (GCC), acknowledged the invaluable presentations provided by the experts and country representatives at the meeting. Mr. Al Sharhan in his intervention shared information on what the GCC is doing on cybersecurity and specific activities that the

[33] http://www.itu.int/ITU-D/cyb/events/2008/doha/docs/krotoski-regional-international-cooperation-doha-feb-08.pdf

GCC is planning to undertake in the future. He noted that since 2004 the GCC have been actively encouraging countries in the region to set up computer emergency response teams (CERTs) and a meeting for GCC countries was held in Qatar to discuss cybersecurity for the region. As a result, a Memorandum of Understanding (MoU) was adopted where a draft project for a regional cybersecurity center/CERT, was discussed. However, the proposal for a GCC-wide CERT was not adopted at the meeting.

66. It was noted at this GCC meeting that if the CERT is meant to be a common center for all GCC countries, another process for financing the center would be needed as the budget for the center could not be supported by only one government. Therefore, as an interim solution, it was also proposed that Q-CERT be authorized to establish bilateral agreements between Qatar and other GCC countries to assist in building CERT capabilities. Unfortunately, this proposal was also not successful and in order to move forward it was agreed at a ministerial meeting that a committee be set up to establish guidelines for this collaboration and that Qatar be responsible for this. Mr. Al Sharhan mentioned that the GCC countries are very excited about the project to establish a CERT for the GCC countries, and its future implementation will be a true achievement for the GCC. Mr. Al Sharhan concluded by mentioning that the GCC is still waiting for input from the Member States as to what approach to be taken for a GCC CERT.

67. Khaled Foda, Head of IT Section, Telecommunication and IT Department, League of Arab States (LAS) shared some information on how LAS Member States have approached cybersecurity-related issues. Mr. Foda mentioned that the Arab countries were among the first regional groups that recognized the importance of adopting and implementing a strategy at the regional level to build the information society. This resulted in the adoption of a strategy document for the Arab community on communications and information technology in 2001 at a summit in Amman. The Arab countries also contributed actively to the two phases of the WSIS. With technologies changing and evolving rapidly, Arab countries have realized the need to formulate and approve a new document to enable the countries to work even more effectively at national and regional levels. As there is a need to further strengthen the interaction between the various parties concerned, taking into account relevant regional and international development in this area, during the past year, countries have drafted the “Arab Strategy for Communications and Information Technology - Building the Information Society 2007-2012”, which will be presented at the forthcoming summit in Damascus, Syria in March 2008.

68. The strategy seeks to achieve three main strategic objectives, namely: 1) to create a competitive market for the Arab information society, as part of the global information society; 2) to achieve universal access and improve the quality of services to the Arab citizen using ICTs; and 3) to further develop the IT and communications industry in order to create new job opportunities and new expert services and opportunities. Building confidence and security in the use of ICT is an integral part of these activities. Information security, network security, data protection and privacy are prerequisites for the development of the information society and building confidence among users. Mr. Foda further mentioned that the LAS will try to implement these goals: a) by contributing to the securing and managing of digital copyright on the Internet and binding formulation of policies to combat infringement of intellectual property rights; b) through cooperation at the international level to fight crimes in cyberspace and the misuse of ICTs; c) through the development of data protection legislation to ensure the protection of privacy for the Arab citizen; d) through providing information security and networks to ensure the user's privacy; and e) by passing laws and legislation criminalizing the penetration of networks. The selection of projects that seek to achieve these strategic goals and objectives is currently under way. The Arab countries have begun studying different approaches and options, with proposals from Morocco and Kuwait, and one, Mr. Foda mentioned, is for an Arab Center for Incident Response (Arab CERT), proposed by Qatar.

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

69. The final session of the meeting, facilitated by Robert Shaw, ICT Applications and Cybersecurity Division, ITU Telecommunication Development Sector (ITU-D), 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. The participants agreed on the following outcomes from the events (see the full Doha Declaration on Cybersecurity in Annex 1 below):

- Recognized that improving cybersecurity is a global problem and that each country must undertake action to join and support international efforts to improve cybersecurity.
- Recognized the initiatives, actions and approaches that have worked in a number of countries and in other regions and the efforts of the ITU and other organizations to compile a set of “best practices” and develop tools which can support national efforts within the Arab region.
- Recognized that the ITU Cybersecurity/CIIP Framework offers a useful guide for raising awareness and initiating and/or reviewing national action as it helps to ensure consistency and compatibility of action among nations.
- Recommended that the ITU Cybersecurity/CIIP Framework and related resources and toolkits be finalized as soon as possible and made available in all ITU working languages, with particular attention to Arabic to support efforts in the region.
- Encouraged each country in the region to utilize the Framework and related ITU self-assessment toolkit

as a means to develop their institutions, policies and relationships for cybersecurity and protecting critical information infrastructures.

- Recognized that some countries in the region may need support and assistance to implement the Framework and use the ITU National Cybersecurity/CIIP Self-Assessment Toolkit and requested that ITU-D consider ways to provide this support.
- Agreed that each country in the region should, if it has not already done so, develop an incident management capability (CSIRT/CERT) with national responsibility and use current examples and best practices of CSIRTs/CERTs in the region when developing national capabilities.
- Agreed that an important component of developing a national framework is joining regional and international efforts to promote a culture of cybersecurity.
- Emphasized the importance of developing regional cooperation initiatives and resources that can provide examples of best practices and training and education opportunities and develop models for capacity building that can be adapted to each country's needs in the region.
- Requested ITU-D in partnership with regional organizations and national administrations to undertake initiatives necessary to follow-up on the results of the meeting and to provide updates on progress and regional cooperation. In these follow-up initiatives, participation should be encouraged by additional participants identified in the Framework (e.g., all relevant ministries, business and other organizations).
- Expressed their appreciation to ictQATAR/Q-CERT and the ITU for their support and facilitation of the meeting.

Meeting Closing

70. In his closing remarks on behalf of ictQATAR and Q-CERT, Michael Lewis, Deputy Director, Q-CERT, Qatar hoped that the workshop had proven useful for the workshop participants, with fruitful and engaging discussions. Mr. Lewis noted that directly following the three day ITU Regional Workshop on Frameworks for Cybersecurity and CIIP on Thursday, 21 February 2008, a one day Cybersecurity Forensics Workshop was being held. More information about the Cybersecurity Forensics Workshop, including links to presentations made during the workshop, can be found on the following link: www.itu.int/ITU-D/cyb/events/2008/doha/presentations.html#forensics[34]

71. Ebrahim Al-Haddad, Head, ITU Regional Office for Arab States, thanked everyone who had directly or indirectly contributed to the success of the ITU Regional Cybersecurity Forum. He relayed special thanks to the local hosts, for their outstanding work in making this regional cybersecurity workshop a highly successful event. Mr. Al-Haddad also thanked the workshop speakers for taking time out of their busy schedules to share their experiences and expertise with the meeting participants. Finally, Mr. Al-Haddad thanked the meeting interpreters who had provided excellent simultaneous interpretation in English and Arabic during the three day event, as well as the delegates for their attention and active participation and contributions. ITU with its long withstanding 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.

This draft meeting report[35] is currently open for the comments for a period of 30 days after reception and publication on the workshop website. The email address for comments on this draft report, and for comments on the ITU Cybersecurity Work Programme to Assist Developing Countries (2007-2009)[36], is **cybmail(at)itu.int**[37].

For information sharing purposes, all meeting participants will be added to the **cybersecurity-arab-states(at)itu.int**[38] for matters concerning ITU-D cybersecurity-related activities. If you have not participated directly in the workshop, 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**.

[34] http://www.itu.int/ITU-D/cyb/events/2008/doha/presentations.html#forensics

[35] http://www.itu.int/ITU-D/cyb/events/2008/doha/docs/doha-cybersecurity-forum-report-feb-08.pdf

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

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

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

ANNEX 1

ITU Regional Cybersecurity Forum Agreed Output

18-20 February 2008

Doha, Qatar

An ITU Regional Cybersecurity Forum[39] was held 18-20 February 2008 in Doha, Qatar, in collaboration with the Qatar Supreme Council of Information and Communication Technology (ictQATAR) and Q-CERT. Over 80 representatives from 18 countries in the Arab region, experts from outside the region (e.g., Malaysia, USA), and representatives from key regional organizations including the League of Arab States (LAS), Gulf Cooperation Council (GCC), and United Nations Economic and Social Commission for Western Asia (UN-ESCWA), participated in the Forum.

During the three days of this event, cybersecurity and critical information infrastructure protection (CIIP) were examined within the context of the draft "ITU Cybersecurity Framework"[40] being developed in the ITU Development Sector's Study Group 1 Question 22/1. A number of interesting presentations on national experiences and regional initiatives (e.g., LAS, GCC, UN-ESCWA) addressing each element of the framework were discussed, including:

- Developing a National Strategy for Cybersecurity;
- Establishing National Government-Industry Collaboration;
- Deterring Cybercrime;
- Creating National Incident Management Capabilities; and
- Promoting a National Culture of Cybersecurity.

It was recognized that each of these elements form part of a comprehensive national approach to cybersecurity.

A related resource, the draft "ITU National Cybersecurity/CIIP Self-Assessment Toolkit"[41] was also examined. The toolkit is designed to assist national governments to review and understand their existing national approach, develop a baseline in terms of current "Best Practices", identify areas for attention, and prioritize national efforts to address cybersecurity.

The role of government in leading national cybersecurity efforts was discussed as well as the challenges faced within all governments to achieving the necessary actions. Discussions were held on the need to raise awareness among all participants, and of the need to tailor arguments to different audiences, whether they be political arguments to senior leaders, economic arguments to business, or personal safety arguments to individual users.

Discussions were held on the importance of including the private sector and other groups in the development of policy and law in this domain, and in the implementation and operation of a national cybersecurity strategy.

Discussions were held on the importance of reviewing national cybercrime legislation to ensure it addresses threats in cyberspace and learned that the Convention on Cybercrime (Budapest, 2001) which offers an internationally developed basis for examining existing national cybercrime law and for determining what new substantive, procedural and mutual assistance provisions are needed in national cybercrime law.

Discussions were held on the importance of developing a national focal point for cyber incident management with the mission of watch, warning, investigation, response and recovery. Such a national focal point can serve to maintain collaboration within government, between the government and the private sector, and with international partners.

Discussions were held on the necessity of promoting a national culture of cybersecurity to ensure that all users, owners, and operators of information systems and networks know their responsibilities in regard to security and have the tools to take action appropriate to their roles.

[39] The title of the event was "Workshop on Frameworks for Cybersecurity and Critical Information Infrastructure Protection (CIIP)" described at http://www.itu.int/ITU-D/cyb/events/2008/doha/.

[40] http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-draft-cybersecurity-framework.pdf

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

Doha Declaration on Cybersecurity – ITU Regional Cybersecurity Forum[42]

At the conclusion of this event, the participants agreed on the following outcomes:

- Recognized that improving cybersecurity is a global problem and that each country must undertake action to join and support international efforts to improve cybersecurity.
- Recognized the initiatives, actions and approaches that have worked in a number of countries and in other regions and the efforts of the ITU and other organizations to compile a set of "best practices" and develop tools which can support national efforts within the Arab region.
- Recognized that the ITU Cybersecurity/CIIP Framework offers a useful guide for raising awareness and initiating and/or reviewing national action as it helps to ensure consistency and compatibility of action among nations.
- Recommended that the ITU Cybersecurity/CIIP Framework and related resources and toolkits be finalized as soon as possible and made available in all ITU working languages, with particular attention to Arabic to support efforts in the region.
- Encouraged each country in the region to utilize the Framework and related ITU National Cybersecurity/CIIP Self-Assessment Toolkit as a means to develop their institutions, policies and relationships for cybersecurity and protecting critical information infrastructures.
- Recognized that some countries in the region may need support and assistance to implement the Framework and use the ITU National Cybersecurity/CIIP Self-Assessment Toolkit and requested that ITU-D consider ways to provide this support.
- Agreed that each country in the region should, if it has not already done so, develop an incident management capability (CSIRT/CERT) with national responsibility and use current examples and best practices of CSIRTs/CERTs in the region when developing national capabilities.
- Agreed that an important component of developing a national framework is joining regional and international efforts to promote a culture of cybersecurity.
- Emphasized the importance of developing regional cooperation initiatives and resources that can provide examples of best practices and training and education opportunities and develop models for capacity building that can be adapted to each country's needs in the region.
- Requested ITU-D in partnership with regional organizations and national administrations to undertake initiatives necessary to follow-up on the results of the meeting and to provide updates on progress and regional cooperation. In these follow-up initiatives, participation should be encouraged by additional participants identified in the Framework (e.g., all relevant ministries, business and other organizations).
- Expressed their appreciation to ictQATAR/Q-CERT and the ITU for their support and facilitation of the meeting.

****

[42] The Doha Declaration on Cybersecurity can also be found online: http://www.itu.int/ITU-D/cyb/events/2008/doha/docs/doha-regional-cybersecurity-forum-output-20-feb-08.pdf