

Regional Workshop on Frameworks for Cybersecurity and Critical Information Infrastructure Protection (CIIP)

Document RWH/2007/01-E
17 September 2007 Rev 1.0
Original: English

Meeting Report : Regional Workshop on Frameworks for Cybersecurity and CIIP Hanoi, Viet Nam, 28-31 August 2007

Please send any comments you may have on this meeting report to [cybmail\(at\)itu.int](mailto:cybmail(at)itu.int)

Purpose of this Report

1. The Regional Workshop on Frameworks for Cybersecurity and Critical Information Infrastructure Protection (CIIP) was held in Hanoi, Viet Nam, 28-31 August 2007. The workshop was the first of a series of regional cybersecurity capacity-building events jointly organized by the ITU Telecommunication Development Sector (ITU-D) and ITU Telecommunication Standardization Sector (ITU-T). The workshop aimed to identify the main challenges faced by countries in the Asia-Pacific region in developing frameworks for cybersecurity and CIIP, to consider best practices, share information on technical standards and 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. Approximately 100 people participated in the event, from countries in the Asia Pacific region and other parts of the world. Full documentation for the workshop, including the final agenda and all presentations made, is available on the event website at www.itu.int/itu-d/cyb/events/2007/hanoi/. This meeting report summarizes the discussions throughout the four days, provides a high-level overview of the sessions and speaker presentations, and presents common understandings and positions reached at the event.

Regional Workshop on Frameworks for Cybersecurity and Critical Information Infrastructure Protection in Hanoi, Viet Nam, 28-31 August 2007

3. As background for the event, at the start of the 21st century, modern societies have a growing dependency on information and communication technologies (ICTs) that are globally interconnected. However, this interconnectivity also creates interdependencies and risks that need to be managed at national, regional and international levels. Enhancing cybersecurity and protecting critical information infrastructures are essential to each nation's security 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 framework for cybersecurity and critical information infrastructure protection requires a comprehensive approach. This event discussed key elements in developing frameworks for cybersecurity and critical information infrastructure protection.

Meeting Opening and Welcome

4. The Regional Workshop on Frameworks for Cybersecurity and Critical Information Infrastructure Protection was opened with a welcoming address by Vice-Minister Vu Duc Dam from the Vietnamese Ministry of Information and Communications (MIC). Vice-Minister Dam highlighted that cybersecurity and critical information infrastructure protection are very important challenges to the Information Society that cannot be answered without concrete action. He invited workshop participants to engage in fruitful and focused discussion during the four day long event.
5. This welcoming address by MIC was followed by [opening remarks](#)¹ made by the ITU Senior Adviser for Asia and Pacific, Aurora Rubio, on behalf of ITU-D Director Sami Al-Basheer and ITU-T Director Malcolm Johnson. In her opening remarks, Ms. Rubio noted that this workshop presents an excellent opportunity for sharing experiences and best practices on addressing the challenges faced by countries in the Asia-Pacific region in

¹ <http://www.itu.int/ITU-D/cyb/events/2007/hanoi/docs/opening-remarks-BDT-TSB-cybersecurity-workshop-hanoi-28-aug-07.pdf>

developing relevant frameworks as well as increasing awareness on relevant ITU-T Recommendations and other cybersecurity-related activities in the ITU Telecommunication Development and Standardization Sectors. Ms. Rubio invited all participants to take advantage of the presence of the experts speaking at the event as well as all counterparts from countries in the Asia Pacific region and other regions; to actively participate in all the sessions of the workshop by sharing views and experiences; and to raise any questions or issues that participants have regarding on the topics discussed.

Session 1: What is a Framework for Cybersecurity and Critical Information Infrastructure Protection?

6. 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 cybersecurity/CIIP institutional framework structures while others have used a light-weight and non-institutional approach. This session discussed the concept of a national framework for cybersecurity and CIIP and ongoing efforts to elaborate such a framework in the ITU.

7. Robert Shaw, ICT Applications and Cybersecurity Division, ITU Telecommunication Development Sector (ITU-D) acted as the moderator for this session which sought to review, from a broad perspective, different approaches to cybersecurity and CIIP frameworks and their often similar components in order to provide meeting participants with an overview of the issues and challenges involved. Mr. Shaw provided an overview of some of [ITU-D's Activities in the Area of Cybersecurity and CIIP](http://www.itu.int/ITU-D/cyb/events/2007/hanoi/docs/shaw-cybersecurity-ciip-hanoi-28-aug-07.pdf)² and shared details on the [ITU-D Cybersecurity Work Programme for Developing Countries](http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-cybersecurity-work-programme-developing-countries.pdf)³. Some of the ongoing and planned ITU cybersecurity initiatives mentioned 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 on capacity building on frameworks for cybersecurity and CIIP.

8. Mr. Shaw noted that most countries have not yet formulated or implemented a national strategy for cybersecurity and critical information infrastructure protection. Mr. Shaw emphasized that we should avoid duplicating efforts and solicited comments from all parties to make sure that ITU is indeed doing what is most needed by its Member States. He also mentioned that one challenge in moving forward on discussions relating to cybersecurity was finding appropriate mechanisms for different actors to communicate better 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.

9. James Ennis, Department of State, United States of America, in his capacity as the ITU-D Study Group 1 Question 22 Rapporteur, followed with an overview of the activities currently under way in this Study Group for developing [Best Practices for Organizing National Cybersecurity Efforts](http://www.itu.int/ITU-D/cyb/events/2007/hanoi/docs/ennis-best-practices-hanoi-28-aug-07.pdf)⁴. He invited workshop participants and countries to join the Q22/Study Group 1 activities which were initiated at the World Telecommunication Development Conference (Doha, 2006). Mr. Ennis indicated that the Question had a potential duration of up to 4 years (until 2010). The output of the work conducted in the Study Group will be a report on Best Practices for Organizing National Cybersecurity Efforts which governments can use as a guideline when undertaking efforts to initiate and formulate national strategies for cybersecurity and CIIP. Mr. Ennis recognized that today, all critical sectors of society rely on information and communication networks for their stable functioning. In order to achieve a maximum level of security, these systems need to be reliable, secure, and trusted. He highlighted that all countries are affected by this including both developed and developing countries.

10. Based on the work underway in ITU-D Question 22/1, Mr. Ennis introduced a five element framework for building a good national cybersecurity programme. This framework includes: developing a national strategy; building a sound legal foundation to deter cybercrime; developing national incident management capabilities; enhancing collaboration between government and industry; and raising national awareness of the importance of cybersecurity in the country. Mr. Ennis emphasized that the overall coordination of a national cybersecurity program needs to be established at a very high level in national governments.

11. The next speaker, William McCrum, Industry Canada, Canada, discussed in his presentation some of the [Challenges in Developing National Cybersecurity Policy Frameworks](http://www.itu.int/ITU-D/cyb/events/2007/hanoi/docs/mccrum-security-policy-frameworks-hanoi-29-aug-07.pdf)⁵. Given the constantly changing security environment, Mr. McCrum emphasized that maintaining trust and confidence in ICT infrastructures is a true challenge. Critical infrastructures are now dependent on secure ICT infrastructures and as this infrastructure evolves into a converged network platform, this leads to many challenges for interoperability and security. Mr. McCrum pointed out that the more connected we are, the less secure we are. He emphasized that it is not enough to focus on one specific area and hope that this will ensure security in the networks; instead, all different areas critical to cybersecurity must be tackled. Mr. McCrum emphasized that everyone is a stakeholder in the cybersecurity business and everyone has a role to play.

² <http://www.itu.int/ITU-D/cyb/events/2007/hanoi/docs/shaw-cybersecurity-ciip-hanoi-28-aug-07.pdf>

³ <http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-cybersecurity-work-programme-developing-countries.pdf>

⁴ <http://www.itu.int/ITU-D/cyb/events/2007/hanoi/docs/ennis-best-practices-hanoi-28-aug-07.pdf>

⁵ <http://www.itu.int/ITU-D/cyb/events/2007/hanoi/docs/mccrum-security-policy-frameworks-hanoi-29-aug-07.pdf>

12. Mr. McCrum also provided workshop participants with an overview of possible cybersecurity policy framework elements, which included: protecting users and safeguarding ICT infrastructure; establishing a national CSIRT/CERT; establishing cybersecurity best practices for all applications, service and network providers and adopting guidelines for securing ICT infrastructures; promoting cybersecurity information-sharing between stakeholders by organizing round-table exchanges and communities of interest; raising awareness of cyber risks and cybersecurity protection strategies through development of advertising campaigns that alert users to risk and mitigation; and the establishment of hotlines for users to deal with cybersecurity threats, attacks and fraud. He concluded his presentation by highlighting the importance of standards development for cybersecurity in order to accelerate adoption of new technology, ensure interoperability between competing platforms and technology, link supply chains, increase market efficiency, and facilitate regulatory compliance. He noted that the activities of ITU-T Study Group 17 are very important to achieving these goals.

13. Phil Sodoma, Trustworthy Computing Group, Microsoft Corporation followed with his presentation on [Resiliency Rules: 7 Steps for Resiliency in Critical Infrastructure Protection](#)⁶. The purpose of the Resiliency Rules 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/operators can collaboratively pursue a set of core enablers of resiliency and infrastructure.

14. The 7 Steps include: 1) Define goals and roles. Establishing clear goals is central to generate support for cybersecurity by the different stakeholder group while understanding the different roles of the stakeholders promotes coordination, efficiency and trust. 2) Identify and prioritize critical functions. Close collaboration is needed to understand interdependencies involved. Mr. Sodoma encouraged countries to establish an open dialogue to understand the critical functions, infrastructure elements, and key resources necessary for delivering essential services, maintaining the orderly operations of the economy, and helping to ensure public safety. 3) Continuously assess and manage risks as protection is the continuous application of risk management. 4) Establish and exercise emergency plans and improve operational coordination. Emergency response plans can mitigate damage and promote resiliency. 5) Create public-private partnerships. Mr. Sodoma explained why the importance of public-private partnerships should not be underestimated. The creation of trusted relationships is key to information sharing and developing solutions to difficult problems and leveraging the unique skills of government and private sector organizations are necessary to address today's dynamic threat environment. 6) Build security/resiliency into operations as security is a continuous process 7) Update and innovate technology/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.

15. Mr. Sodoma indicated that a role of the government is risk assessment, the role of the public-private partnership is to define what is critical, and the role of infrastructure operators is to prioritize risks. Mr. Sodoma ended his presentation by noting that in the past security in enterprises was seen as a technology issue, but this has changed over the past few years, and it is now widely recognized that a more comprehensive, multi-layered security approach is necessary. He also noted that software created 10 years ago was not created for the current threat environment. Therefore, it is important to always use the latest version of available software and hardware.

Session 2: Development of a National Strategy

16. Increasingly, electronic networks are being used for criminal purposes, or for objectives that can harm the integrity of critical infrastructure and create barriers for extending the benefits of ICTs. To address these threats and protect infrastructures, each country needs a comprehensive action plan that addresses technical, legal and policy issues, combined with regional and international cooperation. What issues should be considered in a national strategy for cybersecurity and critical information infrastructure protection? Which actors should be involved? Are there examples of frameworks that can be adopted? This session, moderated by Vu Quoc Khanh, VnCERT, Viet Nam sought to explore in more detail various approaches, best practices, and identify key building blocks that could assist countries in the Asia-Pacific region in establishing national strategies for cybersecurity and CIIP.

17. In the first presentation in this Session 2 on the Development of a National Strategy, Vu Quoc Khanh, VnCERT, Viet Nam, shared some [Issues in Building National Strategy for Cybersecurity in Vietnam](#)⁷. Mr. Khanh explained that the development of ICTs is progressing well in Vietnam, but so are the threats. The number of incidents is increasing every year in accordance with the global trend, and new viruses appear every month. There is currently no Vietnamese strategy for cybersecurity and CIIP yet, but that the country hopes to have this in place by next year. Main challenges that Vietnam is experiencing in moving forward on establishing a national cybersecurity strategy include: defining the critical infrastructures, putting in place appropriate legislation in order to update the legal environment; and setting up all necessary conditions for implementing the national strategy.

18. Mr. Khanh also noted that there are currently six critical priorities for cybersecurity in Vietnam, including: the establishment of a national cybersecurity response system; a national cybersecurity threat and vulnerability

⁶ <http://www.itu.int/ITU-D/cyb/events/2007/hanoi/docs/sodoma-frameworks-microsoft-hanoi-28-aug-07.pdf>

⁷ <http://www.itu.int/ITU-D/cyb/events/2007/hanoi/docs/khanh-vncert-hanoi-28-aug-07.pdf>

reduction program; a national cybersecurity awareness and training program; securing government's cyberspace; and improving the national legal environment and policy for cybersecurity.

19. Devi Annamalai, Security, Trust and Governance Department, Malaysian Communications and Multimedia Commission (MCMC), Malaysia, followed with a country case study, [National Strategy: Malaysian Experience](#)⁸. Ms. Annamalai shared information with the delegates on Malaysia's strategy for cybersecurity, which includes: comprehensive laws and policies; effective monitoring tools; awareness and education; capacity building, and international collaboration. Ms. Annamalai went into each of these five areas, explaining how Malaysia has reviewed existing laws to take cybersecurity into account and what the country is doing to deal with the problem of spam. In dealing with spam, Malaysia currently has no specific legislation but have recently issued a tender for this research and are actively working towards such a law. Ms. Annamalai talked about some of the ongoing public and private sector related cybersecurity initiatives and the roles of the different stakeholders in Malaysia. Initiatives included the Information Sharing Forum and the Information Network Security Portal (INS) which will serve as a focal point and one-stop information centre on information and network security for the communications and multimedia industry. She also shared insights into the Cyber Security Malaysia initiative which offers research in vulnerability detection, intrusion detection and computer forensic technology, offers security services to the private and public sector and operates MyCERT⁹.

20. In the next presentation, Yuejin Du, CNCERT/CC, People's Republic of China, discussed [National Network Security Capacity Building](#)¹⁰, and provided workshop participants with ideas on how countries can build the capabilities needed to fight online threats. The network security capacity model involves four main "capabilities": taking precautions (capability of 'yu' (预) which includes prevention, early warning, evaluation and detection at an early stage), knowing what is happening (capability of 'zhi' (知) which includes monitoring), controllability (capability of 'kong' (控) which involves emergency response and crisis management), recovering and surviving (capability of 'sheng' (生) which includes recovering from an attack and ensuring survivability of the core). China has already implemented some of these capabilities by creating a national CSIRT (CNCERT), and building a national emergency security framework. In addition Mr. Du mentioned a set of network security and capacity building "elements" and "threats".

21. In the following presentation, Kelly Mudford, Department of Communications, Information Technology and the Arts (DCITA), Australia, discussed the Australian [E-Security National Agenda](#)¹¹. Ms. Mudford outlined the E-Security National Agenda (ESNA), which was established in 2001 to create a secure, trusted electronic operating environment for both the public and private sectors. The ESNA was recently reviewed and has been revised (July 2007) due to substantial changes in the online environment. As a result of the review, three new policy priorities have been established to provide a more holistic approach to e-security.. Ms. Mudford also shared information on some of Australia's awareness raising initiatives targeted at the most vulnerable sector: home users and small and medium sized enterprises (SMEs). These include a national cybersecurity week (a pilot was held in 2006) as a good example of public-private partnerships, the StaySmartOnline.gov.au¹² website, the National E-Security Alert Service, and an e-security Schools Module for primary and secondary school students. Close collaboration with industry was furthermore mentioned as key in implementing the Agenda as was the importance of international cooperation for enhanced global cybersecurity.

22. To draw some major finding from the two first workshop sessions Joseph Richardson, United States of America, with his presentation on [Management Framework for Organizing National Cybersecurity Efforts: Self-Assessment Tool](#)¹³ described the elements of the ongoing ITU work to develop a comprehensive [National Cybersecurity/CIIP Readiness Self Assessment Toolkit](#)¹⁴. The self-assessment tool is based on Q22/1 available framework best practices documents and is intended to assist national governments in understanding existing approaches, comparing the national framework to best practices, identifying areas for attention, and prioritizing national efforts for cybersecurity and CIIP. The toolkit examines the management and policy level for each element of the proposed best practices framework that was [presented](#) by Mr. Ennis in Session 1 of the meeting, namely: national strategy; deterring cybercrime; national incident management capabilities; government-private sector collaboration; and a culture of cybersecurity.

23. Mr. Richardson noted in his presentation that no country is starting at zero when it comes to initiatives for cybersecurity and critical information infrastructure protection. Furthermore, 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 equally important all stakeholders, appropriate to their roles, must be involved in developing a national strategy for cybersecurity and CIIP.

⁸ <http://www.itu.int/ITU-D/cyb/events/2007/hanoi/docs/annamalai-malaysia-national-strategy-hanoi-28-aug-07.pdf>

⁹ <http://www.mycert.org.my/>

¹⁰ <http://www.itu.int/ITU-D/cyb/events/2007/hanoi/docs/du-national-network-security-hanoi-29-aug-07.pdf>

¹¹ <http://www.itu.int/ITU-D/cyb/events/2007/hanoi/docs/mudford-australia-E-security-national-agenda-hanoi-28-aug-07.pdf>

¹² <http://www.staysmartonline.gov.au>

¹³ <http://www.itu.int/ITU-D/cyb/events/2007/hanoi/docs/richardson-cybersecurity-self-assessment-tool-hanoi-28-aug-07.pdf>

¹⁴ <http://www.itu.int/ITU-D/cyb/cybersecurity/>

24. At the end of the first day of the workshop the Ministry of Information and Communications (MIC), Viet Nam, invited all workshop participants to a much-appreciated reception and Vietnamese cultural show.

Session 3: Technical Standards for Cybersecurity

25. Standards-development bodies are an important player in addressing security vulnerabilities in ICTs. Session 3 of the workshop, moderated by Yuejin Du, CNCERT/CC, People's Republic of China, highlighted some of the main activities of standards development organizations (SDOs), focusing on ITU-T, and considering topics such as security architecture, cybersecurity, security management, identity management, security baseline for network operators, and the ICT Security Standards Roadmap initiated by ITU-T Study Group 17.

26. Georges Sebek, Counsellor for Study Group 17, ITU Standardization Bureau (ITU-T), opened the standards discussions with an [Overview of ITU-T Activities](#)¹⁵. Mr. Sebek explained the importance of the work conducted in the ITU-T Study Groups, and highlighted activities of ITU-T Study Group 17 which is the main ITU-T Study Group for security. The ITU-T security building blocks which includes the X.800-series (Security Architecture Framework), X.805, X.1000-series (Telecommunication Security), Y.2700-series (NGN Security), etc. were also explained.

27. Mike Harrop, ITU-T Study Group 17 Rapporteur on Security Frameworks, gave the workshop participants further insight into [ITU-T Network Security Initiatives](#)¹⁶. He showed the context of ITU-T security standards activities in light of the larger security standards arena, highlighted some of key areas of work in SG17 Working Party 2 and SG13 Question 15, and reported on the results achieved through specific SG 17 security projects and outreach activities. For example, the ITU-T Security in Telecommunications and Information Technology Manual¹⁷ provides an overview of existing ITU-T recommendations for secure telecommunications. The Security Compendium¹⁸ is a catalogue of approved ITU-T Recommendations related to telecommunication security. The newly released Security Standards Roadmap¹⁹ (v.2, 2007) is an online security standards resource which has been developed by ITU in collaboration with the European Network and Information Security Agency (ENISA) and the Network and Information Security Steering Group (NISSG). The Roadmap comprises five parts: Part 1 contains information about organizations working on ICT security standards; Part 2 is database of existing security standards; Part 3 lists (or links to) current projects and standards in development; Part 4 identifies future needs and proposed new standards; and Part 5 lists security best practices. Mr. Harrop also mentioned that Study Group 17 is currently establishing a Security Standards Exchange Network (SSEN) to maintain on-going dialogue on key security standardization issues.

28. This was followed with a presentation by Koji Nakao, KDDI, Japan, with an [Overview of Information Security Management Activities Undertaken within ITU-T SG 17 and ISO/IEC JTC1/SC 27](#)²⁰. Mr. Nakao highlighted in his presentation that if there are no appropriate security countermeasures in an organization, the following risks can be assumed: loss of customer service, sales and market share, the loss of revenue, income and financial stability, damage to customer trust and confidence and damage to the organization's image, reputation and brand name as well as non-compliance with legislation. He also introduced workshop participants to the revised Recommendation X.1051 on Information Security Management Guidelines for Telecommunications, which is based on ISO/IEC 27002 and considered in ITU-T SG17 Question 7. Mr. Nakao also provided the workshop participants with a short history of computing and insecurity. As a final piece of advice to meeting participants Mr. Nakao highlighted that Information Security Management should not only be considered by individual organizations, but also be established as a baseline for network providers (telecommunications organizations) and customers.

Session 4: Watch, Warning and Incident Response

29. A key activity for addressing cybersecurity at the national level requires preparing for, detecting, managing, and responding to cyber incidents through 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 to undertake steps toward remediation. This session, moderated by Nandkumar Saravade, NASSCOM, India discussed best practices and related standards in the technical, managerial and financial aspects of establishing national or regional watch, warning, and incident response capabilities.

30. Jason Rafail, CERT/CC SEI, Carnegie Mellon University, United States of America, opened this session with an [Overview of the CERT/CC and CSIRT Community](#)²¹. He emphasized that countries need to ensure that accessibility and sustainability is maintained during an attack on national infrastructure, and national CSIRTs

¹⁵ <http://www.itu.int/ITU-D/cyb/events/2007/hanoi/docs/sebek-overview-ITU-T-hanoi-29-aug-07.pdf>

¹⁶ <http://www.itu.int/ITU-D/cyb/events/2007/hanoi/docs/harrop-network-security-initiatives-hanoi-29-aug-07.pdf>

¹⁷ <http://www.itu.int/pub/T-HDB-SEC.03-2006/en>

¹⁸ http://www.itu.int/dms_pub/itu-t/oth/OA/OD/TOA0D0000090001MSWE.doc

¹⁹ <http://www.itu.int/ITU-T/studygroups/com17/ict/>

²⁰ <http://www.itu.int/ITU-D/cyb/events/2007/hanoi/docs/nakao-overview-ism-activities-hanoi-29-aug-07.pdf>

²¹ <http://www.itu.int/ITU-D/cyb/events/2007/hanoi/docs/rafail-cert-overview-hanoi-29-aug-07.pdf>

have an important role to play in this regard. Being proactive and building a culture of security are key to protecting national information infrastructure. Promoting the creation of national CSIRTs is part of a solution on the national level. National CSIRTs provide a conduit for communications and coordination and a goal could be to establish at least one coordinating CSIRT in every country. There are currently 30 national CSIRTs around the world. Services that the national CSIRTs provide include technical services (such as coordination, alerting services, technical publications, incident analysis, vulnerability analysis, artifact analysis, forensic analysis, training) and non-technical services (such as alerting services, user focused publications, general security and computing information). Mr. Rafail described why partnerships are needed for successful response and prevention of incidents.

31. All parties and stakeholders involved need to better understand how the use of information and communication technologies impact their everyday business/activities. While highlighting that people need to have access and knowledge about available security tools, Mr. Rafail also shared information on some online security training resources and tools that the participants could take back with them to countries. These included: the [Virtual Training Environment \(VTE\)](#)²² which is a library of information assurance and computer forensics best practices, [Secure Coding Training](#)²³ resources targeted at enhancing developer skills and capabilities.

32. Marcelo HP Caetano Chaves, CERT-br, Brazil, with his presentation on [Using Honeypots to Monitor Spam and Attack Trends](#)²⁴ shared information on some of the ongoing CERT-br projects and research. As an example he showed what had been done by his team to understand if Brazil really is as big a source of spam, as media was saying that it was, or if someone was using Brazil as a platform for attacks. In this regard, he shared details on the Brazilian Honeypots Alliance Distributed Honeypots Project²⁵ which aims to increase the capacity of incident detection, event correlation and trend analysis in the Brazilian Internet and the Brazilian SpamPots Project which uses honeypots to measure abuse of end-user machines to send spam. Some upcoming activities for CERT-BR include developing more comprehensive spam analysis using data mining techniques, determining patterns in language, embedded URLs, etc. and a project to propose best practices for ISPs including port 25 management and proxy abuse monitoring. Mr. Chaves emphasized that international cooperation is also high on CERT-br's agenda.

33. Keisuke Kamata, JPCERT/CC, Japan, with his presentation on [JPCERT/CC Activities for Critical Infrastructure Protection](#)²⁶, shared JPCERT/CC's experience related to the effectiveness and usefulness of establishing a national CSIRT/CERT in a country. He noted that the national CSIRT serves as the national point of contact for coordination with international CSIRTs and is very effective in bridging the communication gaps between the private and public sectors, and the different function layers (CSIRT, policy makers, law enforcement, competitors, etc.). Mr. Kamata also highlighted the benefits for national CSIRTs to be part of the regional and international networks such as, *inter alia*, the Forum of Incident Response and Security Teams (FIRST)²⁷ and the Asia Pacific Computer Emergency Response Teams (APCERT)²⁸. Building a global distributed network of operational processes between CSIRT partners and systemic sharing of information and resources using a trusted network is seen as fundamental to minimizing the coordination efforts required.

34. Graham Ingram, AusCERT, Australia, started [his presentation](#)²⁹ by highlighting to workshop participants that in the Internet world we still do not fully understand the full impact of the threat (as a key component of the full internet risk equation of vulnerability x threat x impact = Internet risk). Australia's national CERT, AusCERT provides advice to inform on public policy relating to the Internet and information security issues affecting Australian Internet users. He explained how phishing toolkits and related tools are now easily available for purchase through online markets and how cybercrime today pays more than dealing in drugs. Mr. Ingram noted that while local normal crime is going down, online crimes are constantly increasing emphasizing that we are moving towards a service-based criminal economy with criminal services increasingly available for sale. Mr. Ingram also gave an overview of the rapid development of threats, suggesting that botnets are the cybercrime *killer application* as everything can be done with a botnet and scaling issues are not a problem. He gave the example of a single botnet which had at one measurement point more than 28 million infected machines. Due to the increasing problem with botnets, he suggested that workshop participants should focus their attention on botnets rather than malware and spam in their fight against criminal online activities. Mr. Ingram also shared information on how national CSIRTs/CERTs can make a difference in providing a coordinated national and sector initiatives and response. As deteriorating trust and confidence in the online environment is a key issue going forward, he emphasized that building cross-border capabilities that include all countries and economies is critical for establishing a coordinated and cohesive international response.

²² <http://www.vte.cert.org>

²³ <http://www.cert.org/secure-coding/>

²⁴ <http://www.itu.int/ITU-D/cyb/events/2007/hanoi/docs/chaves-cert-br-hanoi-2-aug-07.pdf>

²⁵ <http://www.honeypots-alliance.org.br/>

²⁶ <http://www.itu.int/ITU-D/cyb/events/2007/hanoi/docs/kamata-jpcertcc-hanoi-29-aug-07.pdf>

²⁷ <http://www.first.org>

²⁸ <http://www.apcert.org>

²⁹ <http://www.itu.int/ITU-D/cyb/events/2007/hanoi/docs/ingram-auscert-hanoi-29-aug-07.pdf>

Session 5: Countering Spam and Related Threats

35. One of the more prominent risks to Internet security is spam, which has mutated from a general annoyance to a broader cybersecurity threat. Spam is now the primary mechanism for delivering viruses that can hijack millions of computers (through zombie botnets) or launching phishing attacks to capture private or corporate financial information. Phishing refers to spam sent with a fraudulent motive - for instance, to gather credit card or personal banking information. Spam also acts as a platform for many other types of scams. A number of counter-measures against spammers - technical, legal, financial, user training - can be used against spammers, but there is a general lack of overall coordination at the international level. This session, moderated by Suresh Ramasubramanian, Outblaze, India, looked at some of the best practices and initiatives that have been launched to counter spam and related threats.

36. Richard Cox, The Spamhaus Project, United Kingdom, with his presentation titled [On the Internet Your Reputation Means Everything](#)³⁰, emphasized that cybersecurity cannot be achieved if the bad guys have unfettered access to a shared network. He discussed the challenges linked to spam and why spam will only stop being a problem when it stops being profitable. He suggested that the most effective way to end spam is for networks - especially backbone networks - to act together to suppress the addresses where the spammers operate.

37. In order to ensure that there are no safe havens where spammers and cyber-criminals can operate anonymously, coordinated action is urgently needed. However, as Mr. Cox pointed out, legislation and loss of revenue are cited as the reason why this does not happen. Therefore, he argued that governments and industry bodies needed to formulate policies that reshaped motivation. Mr. Cox indicated trust and teamwork are essential to dealing with the spammers. Mr. Cox ended his presentation with some pieces of advice to the participants: "On the Internet, nobody knows you're a dog! You and your reputation are based solely on what you do and say!" If any party ignores the concerns from other networks and their users, or if they think that you are ignoring these concerns, it is most likely that they will block traffic from your network or even your country.

38. Suresh Ramasubramanian, Outblaze, India, shared information on the [ITU Botnet Mitigation Toolkit project](#)³¹. The Botnet Mitigation Toolkit³² is a multi-stakeholder, multi-pronged approach to track botnets and mitigate their impact, with a particular emphasis on the problems specific to emerging internet economies. Mr. Ramasubramanian explained what people can do with a botnets, in addition to sending spam as had been mentioned in earlier presentations: Examples included to attack a country's Internet infrastructure, extortion such as threats to launch denial of service attacks to cripple e-commerce websites, conduct identity theft and industrial espionage, steal credit card information, passwords etc. from infected personal computers (PCs), and/or launch stock pump-and-dump scams.

39. Bruce Matthews, Australian Communications and Media Authority (ACMA), Australia, provided an overview of [ACMA's Technological Initiatives in Combating Spam and Enhancing Internet e-Security](#)³³ with details on Australia's five part strategy to combat spam. This strategy includes: strong enforcement of the Australian 2003 Spam Act; targeted education and awareness activities; industry measures; technological initiatives and solutions; and international cooperation. Some of the industry measures to combat spam that he mentioned include an E-Marketing Code of Practice which, as registered by ACMA in March 2005, provides guidance to businesses on responsible e-marketing practices, and the Internet Industry Spam Code of Practice, as registered in March 2006, which specifies measures to reduce the incidence and impact of spam on ISP networks and has close linkages to e-security. Mr. Matthews noted that significant increased funding for ACMA's countering spam and e-security initiatives in Australia have been allocated in 2007.

40. In the area of Australian technological solutions and monitoring, two major ACMA initiatives were described including 1) SpamMATTERS³⁴, enlisting the support of the public in fighting spam through a reporting and forensic analysis system developed by ACMA where Australian email users can report spam to ACMA and delete it with a single click of a mouse, and 2) the Australian Internet Security Initiative (AISI), a cooperative arrangement with Australian Internet service providers to shut down infected computers. AISI collects information on compromised computers, compares the IP addresses of these computers to a list of IP address ranges of Australian ISPs, and advises relevant ISP of the IP address so that the ISP can inform and liaise with the customer to fix the problem. In most cases to date, customers are completely unaware that their computers had been compromised. Mr. Matthews also mentioned that Australia is pleased to support working with ITU on its Botnet Mitigation Toolkit.

Session 6: Legal Foundation, Regulatory Development and Enforcement

41. Appropriate legislation, international legal coordination and enforcement are all important elements in preventing, detecting and responding to cybercrime and the misuse of ICTs. This requires updating of criminal law, procedures and policy to address cybersecurity incidents and respond to cybercrime. As a result, many

³⁰ <http://www.itu.int/ITU-D/cyb/events/2007/hanoi/docs/cox-spamhaus-hanoi-29-aug-07.pdf>

³¹ <http://www.itu.int/ITU-D/cyb/events/2007/hanoi/docs/ramasubramanian-itu-zombie-botnet-mitigation-project-hanoi-29-aug-07.pdf>

³² <http://www.itu.int/ITU-D/cyb/cybersecurity/projects/botnet.html>

³³ <http://www.itu.int/ITU-D/cyb/events/2007/hanoi/docs/matthews-acma-initiatives-hanoi-29-aug-07.pdf>

³⁴ <http://www.spammatters.com>

countries have made amendments in their penal codes, or are in the process of adopting amendments, in accordance with international conventions and recommendations. The session moderator Devi Annamalai from the Malaysian Communications and Multimedia Commission (MCMC) opened the session with an insight into what is currently happening in Malaysia with regard to revising existing laws and developing new legislation to deal with citizen's increasing use of information and communication technologies. The session reviewed various national legal approaches and potential areas for international legal coordination and enforcement efforts.

42. Stein Schjolberg, Moss District Court, Norway, provided an overview of the different players involved in the development of a legal framework for cyber-related crimes with his presentation on the [Global Harmonization of Cybercrime Legislation](#)³⁵. He discussed some of the activities undertaken and tools provided by the United Nation, ITU, the European Union, Council of Europe, the G-8 Group of States, Asian Pacific Economic Cooperation (APEC), Organization of American States (OAS), Association of Southeast Asian Nations (ASEAN) and provided examples from Commonwealth Model Legislation. He posited that the Council of Europe's Convention on Cybercrime, which is currently the main legislative framework available to countries, is not dynamic enough to take into consideration the rapid ongoing changes in the cyber-environment.³⁶

43. Pauline Reich, Waseda University, Japan, followed with details and case studies for some countries in the Asia-Pacific region with her presentation on [Cybercrime Legislation-Worldwide Update 2007](#)³⁷. Ms. Reich noted that most countries in the world have not signed or ratified the Council of Europe Cybercrime Convention, particularly those in the Asia-Pacific region and developing countries. She further highlighted that there is not enough dialog between the technology and law enforcement people, and that she was happy to see the ITU stepping forward to bring these issues to different stakeholders' agendas. She saw an issue in the lack of well-trained people, with the requisite technical skills to deal with cybersecurity and cybercrime-related issues. She also saw an issue with the lack of translators that know both law and technology terminology. Ms. Reich shared insights into case studies in the Asia-Pacific region, including examples from Australia, Cambodia, India, Japan, Malaysia, Republic of Korea, Singapore and Thailand. She said that examples from some countries, like Thailand and Singapore, show what she considered to be good examples of prosecutions made, while emphasizing also that these countries have adopted new legislation to deal with spam. She further emphasized a need for cybersecurity/cybercrime curriculum in law faculties, and more distance learning focused on security so that more people can take part in conferences, meetings, workshops, and other fora.

44. Nandkumar Saravade, NASSCOM, India, talked about [Cybersecurity Initiatives in India](#)³⁸. Mr. Saravade pointed out that there is no perfect law for cyber-related crime that would fit all countries and all different circumstances. Therefore, there is clearly a need for local elaboration of relevant legislation first and then each country can adjust this legislation to legislative guidelines available at regional and global levels. As the involvement of all relevant parties in the process is necessary to adopt legislation, one cannot just adopt a ready-made model law to a country and hope it will work. Mr. Saravade also discussed the good cooperation between the Indian Government and NASSCOM, the main trade body and chamber of commerce of the Indian IT-ITES industry. He introduced the NASSCOM 4E framework for trusted sourcing which includes engagement, education and outreach, enactment, and enforcement. He pointed out the important role of media as a key player in raising cybersecurity awareness and emphasized the need for increased training for people on the ground who have to conduct cyber-investigations. He ended his presentation with examples and photos from different cybersecurity initiatives in India (which included everything from daily activities at the Bombay stock exchange, public awareness raising campaigns, essay competitions, to the inclusion of Bollywood film stars in Indian cybersecurity events).

45. Some potential discussed outcomes from the session on Legal Foundation, Regulatory Development and Enforcement included:

- Establishment of a common set of legal principles to provide the basis for national cybersecurity legal frameworks. These principles should promote the sharing of information between authorities with responsibility for addressing cybercrime. Legislation based on these principles should facilitate international cooperation in fighting cyber crime.
- Development of a set of guidelines to assist the establishment of cybercrime legislation. These guidelines would be developed on the basis of an agreed set of principles. This set of guidelines should be particularly targeted at assisting developing economies in constructing legislation in a timely manner.
- Cybercrime legislation should be developed in a wholistic, integrated manner with other legislation, particularly privacy legislation.
- Given the Internet's borderless nature, consideration could be given to developing cross-border legislation and/or laws that have extra-territorial character.
- There must be comprehensive, targeted and efficient education of all parties involved in enacting or implementing legislation.

³⁵ <http://www.itu.int/ITU-D/cyb/events/2007/hanoi/docs/schjolberg-harmonization-of-legislation-hanoi-30-aug-07.pdf>

³⁶ <http://www.cybercrimelaw.net>

³⁷ <http://www.itu.int/ITU-D/cyb/events/2007/hanoi/docs/reich-cybercrime-legislation-hanoi-30-aug-07.pdf>

³⁸ <http://www.itu.int/ITU-D/cyb/events/2007/hanoi/docs/saravade-cybersecurity-initiatives-in-india-hanoi-30-aug-07.pdf>

Session 7: Government/Industry/Standardization Development Organizations Collaboration

46. Industry/government partnerships are founded upon mutual benefit and a clear understanding of roles and responsibilities. A fundamental element of successful industry-government partnerships is trust which is necessary for establishing, developing and maintaining sharing relationships between the private sector and government. The success of industry-government partnerships is dependent on all participants deriving value from the particular partnership. By providing an understanding of each party's roles and responsibilities in cybersecurity and participating in reciprocal information sharing, industry-government partnerships can mitigate and reduce risk and implement a more comprehensive approach to cybersecurity. This session, moderated by William McCrum, Industry Canada, discussed the industry/government partnerships and gave examples and details of some partnerships in which the session speakers were actively involved. Mr. McCrum underscored in both his presentations the importance of best practices, standards and close collaboration.

47. Mike Harrop, Cottingham Group, Study Group 17 Rapporteur on Security Frameworks, shared information on different types of partnership in his presentation on [Standards for Cybersecurity - The Need for Sector Collaboration](#). Mr. Harrop considered the specific needs that both the public and private sector have when it comes to standards. Highlighting that in both cases the demand for standards is driven by specific business requirements and objectives. He pointed out that the private sector needs standards to support or drive competitive positions, meet market demand for standards-compliant products, and to support efficient internal operations. He noted that a dominant supplier can often set its own proprietary standards and use these to disadvantage other suppliers. On the other hand, the public sector needs standards-based products to mitigate product incompatibilities and often requires standards for the "public good" or may have procurement policy or international treaty requirements for standards-based products and services.

48. Mr. Harrop pointed out that closer and improved collaboration between public and private sectors is critical to the success of any national cybersecurity and CIIP strategy. In order to improve collaboration, Mr. Harrop proposed a number of measures that needed to be addressed. The need for improved trust relationships between parties so that information can be exchanged in confidence ensuring that information on threats, attacks and vulnerabilities is relayed to people who can respond in timely manners, was one suggestion. Another included better incident response from business and making sure that businesses reported vulnerabilities and breaches to incident centres promptly. This required that business knows how and to whom to report incidents. Mr. Harrop also emphasised the need to reduce vulnerabilities due to poor private user end systems by encouraging better software and filtering by ISPs, as well as the increased need for cybersecurity metrics and research.

49. Graham Ingram, AusCERT, Australia provided an insight into how collaboration and networking functions in the CSIRT/CERT community functions and how different stakeholders play very effective roles for improved incident reporting and action. He provided an insight into the activities of APCERT, the Asia Pacific Computer Emergency Response Team, which is a coalition of CSIRTs aiming to encourage and support the activity of CSIRTs in the region. APCERT currently involves 20 teams in 14 economies, and the focus of its activities is on what is happening, how to stop incidents, and how to prevent it from happening again.

50. It was emphasized that 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.

Sessions 8: Promoting a Culture of Cybersecurity

51. Considering that personal computers and mobile phones are becoming ever more powerful, that technologies are converging, that the use of ICTs is becoming more and more widespread, and that connections across national borders are increasing, all participants who develop, own, provide, manage, service and maintain information networks must understand cybersecurity issues and take action appropriate to their roles to protect networks. This session, moderated by Marilyn Cade, ICT Strategic Consulting, United States of America, explored the concept of promoting a culture of cybersecurity, and looked closer at some of the roles of the different stakeholders in making this a reality.

52. Christine Sund, ICT Applications and Cybersecurity Division, ITU Telecommunication Development Sector (ITU-D), in her presentation [Promoting a Culture of Cybersecurity](#)³⁹ 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) on the "Creation of a global culture of cybersecurity", and further elaborated on in UN Resolution 58/199 (2004) on the "Promotion of a global culture of cybersecurity and protection of critical information infrastructures". These elements included awareness, responsibility, response, ethics, democracy, risk assessment, security design and implementation, security management, and reassessment. Member States and all relevant international organizations were asked to address and take these elements into account in the preparations for the two phases on the World Summit on the Information Society (WSIS)⁴⁰ in 2003 and 2005. The outcome documents from the two WSIS phases further emphasized the

³⁹ <http://www.itu.int/ITU-D/cyb/events/2007/hanoi/docs/sund-promoting-a-culture-of-cybersecurity-hanoi-30-aug-07.pdf>

⁴⁰ <http://www.itu.int/wsisis/>

importance of building confidence and security in the use of ICTs and countries' commitment to promoting a culture of security.

53. 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 ICT; 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, 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 the various 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. As cybersecurity is at its core a shared responsibility, Ms. Sund ended her presentation with some background information on the recently launched ITU initiative, the [Global Cybersecurity Agenda](#)⁴¹.

54. Marco Gercke, Germany, in his subsequent [presentation](#)⁴² highlighted some of the challenges that developing countries face in their fight against cybercrime with details on the forthcoming 2007 ITU publication "Understanding Cybercrime: A Guide for Developing Countries". He also elaborated on national, regional and international cybercrime legislation in promoting a global culture of cybersecurity. Mr. Gercke noted that finding adequate solutions to respond to the threat of cybercrime is a major challenge for developing countries. The development and implementation of a national strategy for cybersecurity including fighting cybercrime requires time and can prove to be quite expensive which may prevent countries from taking necessary steps to improve security. Therefore, he emphasized that it is important to point out that risks related to weak protection measures can easily affect the societal and business environment in developing countries in critical ways. This, in turn, can make developing countries an even more interesting place for criminals to operate from, and as a result, negatively influence the reputation of the market place. He noted that often starting from a blank slate, developing countries have a unique opportunity to bring their cybercrime strategies in line with necessary standards right from the start.

55. Nguyen Chi Cong, Vietnam Data Communication Company (VDC), provided an overview of VDC's activities and responsibilities as the largest ISP in Vietnam with his presentation on [ISP's Role in Promoting a Culture of Cybersecurity](#)⁴³. Mr. Cong shared details on some of the challenges that VDC faces in protecting the growing Vietnamese economy and its Internet users against cyber-attacks. Ensuring that confidential information is kept secure and that network configurations and business data are only shared with trusted parties as well as ensure that systems and services are always available, are major challenges in today's environment. Mr. Cong also shared with the participants some of VDC's protective measures and responsibilities as the main ISP in Vietnam. These included providing best services for customers through 24/7 availability, providing Internet services to remote areas, providing Internet for schools, sponsorship activities, and implementing assignments on behalf of the Vietnamese Government.

Session 9: Regional and International Cooperation

56. Aurora Rubio, Senior Adviser, ITU Area Office in Jakarta, Indonesia, and Georges Sebek, Counsellor for Study Group 17, ITU Standardization Bureau (ITU-T), in their joint presentation talked about the important role of [Regional Contributions to ITU's Work](#)⁴⁴. In the same session Kelly Mudford, Department of Communications, Information Technology and the Arts (DCITA), Australia, presenting on behalf of APEC TEL Security and Prosperity Steering Group (SPSG), provided an overview of [APEC TEL's regional activities and collaborative cybersecurity initiatives](#)⁴⁵.

Round Table Information Exchanges

57. At the end of each day, the workshop participants broke into smaller groups to allow participants to discuss the programme topics of the day in a smaller roundtable format under the overall guidance of the workshop organizers. An expert for each of the topics moderated the discussions to ensure that all participants were given the opportunity to share their country specific experiences and ask questions from the specific experts involved in the discussions at each table. During the four day long workshop, the smaller groups discussed seven different topics:

⁴¹ <http://www.itu.int/ITU-D/cyb/events/2007/hanoi/docs/cybercurity-agenda-background-information.pdf>

⁴² <http://www.itu.int/ITU-D/cyb/events/2007/hanoi/docs/gercke-guide-hanoi-30-aug-07.pdf>

⁴³ <http://www.itu.int/ITU-D/cyb/events/2007/hanoi/docs/cong-vdc-hanoi-30-aug-07.pdf>

⁴⁴ <http://www.itu.int/ITU-D/cyb/events/2007/hanoi/docs/rubio-sebek-itu-regions-hanoi-31-aug-07.pdf>

⁴⁵ <http://www.itu.int/ITU-D/cyb/events/2007/hanoi/docs/APECTEL-hanoi-31-august-07.pdf>

- What is a Framework for Cybersecurity and Critical Information Infrastructure Protection?, was moderated by James Ennis, Department of State, United States of America, and ITU-D Study Group 1 Question 22 Rapporteur
- Development of a National Strategy, was moderated by Joseph Richardson
- Technical Standards for Cybersecurity, was moderated by Georges Sebek, Counsellor for Study Group 17, ITU Standardization Bureau (ITU-T).
- Watch, Warning and Incident Response, was moderated by Jason Rafail, CERT/CC SEI, United States of America
- Spam and Related Threats, was moderated by Suresh Ramasubramanian, Outblaze, India
- Legal Foundation, Regulatory Development and Enforcement, was moderated by Bruce Matthews, Australian Communications and Media Authority (ACMA), Australia
- Promoting a Culture of Cybersecurity, was moderated by Marilyn Cade, ICT Strategic Consulting, United States of America

58. Before ending the workshop in the afternoon, the groups each reported back to the meeting participants and provided a brief summary of the topics discussed and main challenges identified. The findings and common understandings that emerged during these discussions were later summarized in Session 10 of the meeting. Details on these are highlighted in Session 10 below.

Session 10: Wrap-Up, Recommendations and the Way Forward

59. The final session of the meeting, jointly facilitated by Phan Tam, International Cooperation Department, Ministry of Information and Communication (MIC), Viet Nam, and Robert Shaw, ICT Applications and Cybersecurity Division, ITU Telecommunication Development Sector (ITU-D), provided a summary of the different sessions presented during the workshop and posed questions about what future strategies, solutions, partnerships, frameworks are now need to move forward on these discussions related to frameworks for cybersecurity and critical information infrastructure protection.

60. Four main common understandings and positions were identified by the meeting speakers and participants. These included:

- A. The Need for National Framework(s);
- B. The Need for Capacity Building and Education/Awareness;
- C. The Need for Enhanced Cooperation at Local, National, Regional and International Levels;
- D. The Need for Technical Standards and Best Practices.

These common understandings are discussed in more detail below.

61. **A. The Need for National Framework(s)** : Each country should take into consideration the development of a national framework for cybersecurity and critical information infrastructure protection (national framework) that includes, inter alia: a national strategy; adoption of appropriate legal frameworks including deterring cybercrime; incident management; government-private sector collaboration; and the development of a culture of cybersecurity. In order to achieve the development of a national framework, there is a need for high- level political support for the development of the national framework.

62. Participants in the development of the national framework could include relevant ministries, government agencies, and a broad and diverse participation from the private sector, including business, other organizations, and individual users, each according to their relevant roles.

63. **B. The Need for Capacity Building and Education/Awareness** : Capacity building and education/ awareness are required to support each participant in their respective responsibilities and roles. Each country and different stakeholders will have different needs, and will be at different levels. Therefore, the training and resources should be flexible enough to be adaptable to unique situations and needs of the country and its relevant participants.

64. **C. The Need for Enhanced Cooperation at Local, National, Regional and International Levels:** Enhanced cooperation will be needed both among participant groups, and across sectors; e.g. government and private sector; law enforcement and ISPs, etc., appropriate to their roles. Cooperative efforts will be dynamic, and will vary according to the circumstances. For example, law enforcement and CSIRTS may require ongoing cooperative interaction in incident mediation and resolution. ISPs and law enforcement may primarily interact around incident reporting and investigations. Other flexible interaction models may emerge. Efforts to educate all participants may occur on a more consistent and ongoing basis. Enhanced cooperation initiatives are needed at national, regional, and international levels, and will cross the full range of technical training, experience sharing, and incident investigation, cooperation in legal remedies, user awareness, and policy making.

65. **D. The Need for Technical Standards and Best Practices:** Development of appropriate technical standards and best practices is important to the successful implementation and operation of national strategies and will

facilitate regional and international cooperation initiatives. There is a need for increasing awareness of existing and emerging technical standards from the broad set of relevant standards development organizations (SDOs) and best practice approaches in policy and procedures, which may include, inter alia, training in investigatory techniques, cyberspace forensics, how to set up or manage a CSIRT, examples of successful user awareness programs, etc. be developed across all elements of the national framework.

66. Some overarching approaches and specific activities identified by the participants and speakers included:

- Designing model examples for convening a national framework development process, including identifying potential categories of participants, outline of a national framework, etc.
- Identifying a core set of activities in the form of a 'check list' or model framework examples, that countries can use to assess their cybersecurity readiness, and identify areas for enhancement;
- Facilitating information sharing, knowledge and know how transfer among countries, both governmental and private sector, ISPs, appropriate intergovernmental entities, etc.
- Facilitating interactions with and among experts and expert entities from relevant areas identified in the national framework, such as legal, technical, etc.
- Developing resources that provide examples of best practices; training and education opportunities;
 - Identify relevant standards; and publish user friendly guides with translation and easy to use descriptions of how to implement standards and best practices.
 - ITU Resolution 123 (Rev. Antalya, 2006) relates specifically to "Bridging the standardization gap between developing and developed countries".
 - Such efforts should include ITU-T SG 17, ITU-T SG 13, other relevant Standards Development Organizations (SDOs), such as W3C and IETF, regarding relevant and applicable standards.
- Developing models of capacity building resources that can be adapted to country needs.

67. It was also mentioned that balance is needed between diversification, competition, and coordination on activities undertaken by various stakeholders. Maximizing benefits and making best use of limited resources should be a key goal. Furthermore, the usefulness of and need for a comprehensive calendar of cybersecurity related events worldwide on an ITU website, to which stakeholders could provide updates, was expressed by some of the workshop participants.

Meeting Closing

68. Vu Quoc Khahn, VnCERT, Ministry of Information and Telecommunications (MIC), Viet Nam provided some closing remarks to end the four day long event. He thanked the workshop participants and speakers for taking time out of their busy schedules to travel to Hanoi to take part in the workshop. He re-iterated that Vietnam was pleased to have hosted this regional workshop which is the first in a series of regional cybersecurity events jointly organized by the ITU Telecommunication Standardization and Development Sectors.

69. In her [closing remarks](#)⁴⁶, on behalf of ITU-D Director Sami Al-Basheer and ITU-T Director Malcolm Johnson, ITU's Aurora Rubio, thanked the local Vietnamese hosts for their outstanding work in making this a highly successful workshop. She relayed on special thanks to the Ministry of Information and Communications (MIC) of Vietnam for their excellent hosting of the workshop; VNCERT for their cooperation in the planning and organization of this event and for providing excellent facilities which ensured the efficient conduct of the workshop; all workshop speakers for taking time out of their busy schedules to share their experiences and expertise with the meeting participants; all workshop delegates for their attention and active participation and contribution; the Government of Australia for their financial support for this event; and Vettel, McAfee, VNPT, MobiFone, EVN Telecom and VDC for their sponsorship.

70. As the main facilitator for WSIS Action C5 dedicated to building confidence and security in the use of ICTs, and with its long withstanding activities in the standardization and development of telecommunications, it was emphasized that ITU will 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. With the goal of achieving a common understanding amongst all the concerned parties, identifying how the issues could be addressed globally and agreeing on concrete actions.

⁴⁶ <http://www.itu.int/ITU-D/cyb/events/2007/hanoi/docs/closing-remarks-BDT-TSB-cybersecurity-workshop-hanoi-28-aug-07.pdf>

The email address for comments on this meeting report, and for comments and questions related to the ITU Cybersecurity Work Programme for Developing Countries (2007-2009)⁴⁷, is [cybmail\(at\)itu.int](mailto:cybmail@itu.int). For information sharing purposes, all meeting participants will be added to [cybersecurity-asia-pacific\(at\)itu.int](mailto:cybersecurity-asia-pacific@itu.int)⁴⁸ mailing list and related discussion forums 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](mailto:cybmail@itu.int).

⁴⁷ Please send any comments you may have on the workshop report to cybmail@itu.int

⁴⁸ Regional ITU cybersecurity mailing list: cybersecurity-asia-pacific@itu.int. Please send an e-mail to cybmail@itu.int to be added to the mailing list.