BUILDING THE INFORMATION SOCIETY

3rd Facilitation Meeting for WSIS Action Line C5: Building confidence and security in the use of ICTs

ITU Headquarters, Geneva, 22 -23 May 2008

Document ALC5/2008
Meeting Report

02 June 2008

Original: English

Meeting Report

Purpose of this Report

1. The Tunis Phase of the World Summit on the Information Society (WSIS) has nominated the International Telecommunication Union (ITU) as the facilitator for Action Line C5, dedicated to Building Confidence and Security in the Use of Information and Communication Technologies (ICTs). The first C5 facilitation meeting was held in Geneva on 15-16 May 2006. The second C5 facilitation meeting was held during the cluster of WSIS-related meetings, taking place through 14 to 25 May 2007 in Geneva.
The third facilitation meeting also took place in Geneva.

In accordance with its role as facilitator for this Action Line, this report was prepared by ITU Secretariat. It contains a summary of the presentations and discussions that took place during the two days of the meeting and also provides a high level overview of the six sessions and presentations by the speakers, panellists and moderators.
It also highlights some proposals aimed at making progress towards the goals of WSIS Action Line C5.

Overview of the Meeting

2. A total of 125 participants from governments, industry, international organizations, academia and civil society attended the two-day meeting. Participants from 39 different nationalities, 22 industry experts and 50 participants representing international organizations, NGOs, and academia attended the meeting.
Interactive panel sessions on current and emerging threats and solutions were the focus of the first day on 22 May. Multi-stakeholder panels of experts from governments, industry, international organizations, academia and civil society debated and exchanged views on current and emerging cybersecurity issues and solutions. Day 1 also included open and dynamic discussions with the participants.
The second day, 23 May, was dedicated to presentations by stakeholders on initiatives followed by discussions on identifying possible goals and targets and an exchange of views on mechanisms for performance measurement and reporting towards progress in building confidence and security in the use of ICTs.

The meeting was webcast live in audio/video and the archives are available for download in mpeg4 / ITU-T H.264. Full documentation for the meeting, including the final agenda, all presentations, meeting contributions and biographies is available on the event website at http://www.itu.int/osg/csd/cybersecurity/WSIS/3rdMeeting.html.

The agenda for the meeting was developed with the collaboration of the Geneva Security Forum (GSF).

Session 1: Opening remarks and Overview of the Sessions

Opening and Welcome Remarks

3. The third facilitation meeting for WSIS action line C5 was opened by ITU Deputy Secretary-General, Mr. Houlin Zhao, who stated that security and confidence in the use of ICTs is the top priority for the ITU. It is every person's fundamental right to communicate. The misuse of ICTs for criminal purposes is increasing. Cyberattacks are becoming more sophisticated. Cybercriminals are becoming more organised, extending their operations abroad and obtaining illegal gains through money laundering. It is vital that we become better connected and more organised that the criminals we are fighting.
All three sectors of the ITU have been taking action. ITU however cannot work to resolve these problems alone. Cyberthreats need a coordinated global response. ITU responded to its mandate as facilitator to action line C5 by setting up the Global Cybersecurity Agenda (GCA), including an expert panel from a wide range of different panels.
The GCA has generated significant interest and has caught the attention of world renowned experts from all different areas including industry, government and academia as well as other interest groups.
At the end of this meeting, we should agree on the common targets for fighting cyberthreats to ensure a safer and more secure online environment.
He thanked the Geneva Security Forum for their collaboration with ITU in developing the agenda for the meeting.

Session 1: Managing Cyberthreats – Can we stay one step ahead of the attacker?

4. Mr. Alexander Ntoko, Head, Corporate Strategy Division, ITU

The following sessions will be dynamic and involve lively discussion between the panellists and the experts attending. We want to try to be frank and direct in the discussions. Session one is about managing cyberthreats and if it is possible to stay one step ahead of the attacker.
In 1986 the first virus came out, the 'Brain Virus', in Lahore Pakistan. In May 2000 there was a massive virus the 'I Love You' virus which was estimated to have infected 45 million computers across 20 countries, causing 5-10 billion dollars in damage. We are entering a phase where people have stopped showing off their intellectual capabilities by develop code and are instead trying to inflict harm and profit for financial gains.
This session comprises high-ranking speakers from distinguished backgrounds. Are there some solutions currently in the pipeline that would keep us one step ahead of the attacker?

5. Mr. Eliot Lear, Senior, Consulting Engineer - Security Cisco

The best way to measure the war on cybercrime might best be viewed on economic terms. Is the information society growing, is it successful? The answer is currently yes. We are very positive of the success of the internet. The question is to find out where we can improve. Authentication technology and mechanisms such as ITU-T Recommendation X.509 have provided a good foundation for electronic commerce. One key reference for security standards in use today is the ITU-T Recommendation X.509 for electronic authentication over public networks. X.509, a cornerstone for designing applications related to public key infrastructure (PKI), and is widely used in a wide range of applications from securing the connection between a browser and a server on the web to providing digital signatures that enable e-commerce transactions to be conducted with the same confidence as in a traditional system. Without wide acceptance of the standard, the rise of e-business would have been impossible. These processes have not changed much since they currently appear to satisfy the needs of e-commerce.
In the area of email, we have seen development there as well. A second effort that needs to be understood is about the trustworthiness of the other party. There is a thriving market in the area of reputation service and trusted IDs.
The number of parties involved in a transaction will effect the transaction itself: the buyer, seller, the host server, etc.

6. Mr. Grégoire Ribordy, Co-Founder and CEO, id Quantique, Switzerland

My area of expertise is cryptography which relies heavily on the telecommunication infrastructure to transmit sensitive communication. ID Quantique works on securing ID networks and the information transmitted through it. The problem with conventional cryptography is that it is based on mathematics. It is not necessarily very secure; it only takes a long time to break it. The inventors of this technology proposed a small challenge which was to break the algorithm. Within 3 months, the algorithm was broken. This demonstrates that there is a life-span to the security of the algorithm before it will be broken.
ID Quantique develops cryptography based on quantum technology. Quantum objects are microscopic objects. When information is intercepted, information about the intercept is sent back to the sender.
The first application of this technology was with the Swiss Federal elections which used a secure network based on quantum encryption. It was the first recorded use of such technology. This technology is still currently being improved. It is limited by physical distance at the moment (100

– 200km). The race is ongoing between code makers and code breakers and this is what stimulates further developments in encryption technology.

7. Mr. Paul Nicholas, Principal Security Strategist Manager, Critical Infrastructure Protection Program, Microsoft

The changing nature of attacks has changed the way industry has to think about and deal with attacks. About 48% of attacks have moved into the high-complexity context. The security development lifecycle is based on threat modelling, building software to resist certain types of attacks. When software is developed within the company, it needs to go through this lifecycle. This does not necessarily mean that attacks have ceased. But it means that attacks have shifted from operating system attacks to application based attacks on the web.

Other companies also have a similar process and cooperation between industry players has enabled better understanding on risk management and how governments assess the risks (www.safecode.org).

There is no one solution for fighting such cyberthreats. However risk management and industry partnerships are the most effective tools in combating these threats. By working together, we can really make a big difference in that context.

8. Mr. Ketan Paranjape, Technical Advisor to Intel Chief Technology Officer

Criminal forensics is the training of designers and architects to think like hackers. Learning how people interact how people will use certain applications. User interfaces which are simple to use in order to educate the masses are being developed by Intel. Locking PCs is also another tool often being used by parents. After research, it was understood that consumers wanted a physical lock and key mechanism on their hardware. Online tutorial services and communities are also applications very often used by consumers.

The necessity to secure these sites and other applications is very important. Intel looks into issues such as psychology and sociology in order to determine how consumers use their product and what they want. Human factors play an extremely important role which should not be omitted.

9. Mr. Patrick Amon, Deputy Director, ISIS – EPFL, Switzerland

The systemic problem with internet and computer vulnerabilities in general is not just a technology issue. It is the consequence of a fundamental underlying problem which is economics. The costs of making information systems secure far exceeds the costs of enabling commerce. The interaction between the systems and the users is often the problem. Encryption is the strongest part of the technology. Overall, it is very strong in the sense that increasing the length of the key increases the complexity of cracking the key, unless the mathematics is fundamentally broken.

The difficulty of securing information technology is the measurement of security tools,there are very few '*measurables*'. Building new metrics and factoring those metrics in the pressing of the delivery in the hardware and software will enable better security.

10. Mr. Pradeep K. Khosla, Dean College of Engineering Director, Carnegie Mellon University

Industry is generally the one pushing the technologies. However, no single company can make the system secure on its own. All the companies need to collaborate together in order to pool together their knowledge on different issues.

Open research where the results are widely published and widely disseminated is necessary. The low cost level of entry for a hacker necessitates the open collaboration of governments as well as

industry. There needs to be a holistic view of the problem. The technology, public policy, legal and economic issues are intrinsically linked. There is a lot of overlap between all these issues. We have to think about building systems which are perpetually available where services should not be denied. Many companies are investing a lot of researching in these services.
Between the country that designs an application, the country which fabricates it, and the country that uses it, it becomes difficult to build an entirely trusted system. There is a whole range of issues that opens up concerning this. It is necessary to have technologies that will guarantee security as well as privacy.
Multi-model biometrics will play a very important role in security technologies in the near future. It is one of the few technologies which can almost guarantee it will not be spoofed.
The notion of software liability inevitably will lead to interrogation on whether the user has changed the use the software was initially designed for. Guaranteed packet trace back is another technology which will play an important role in security technologies. The 'Privacy Bird' is software which will read all the privacy policies to ensure it matches your preferred privacy settings before accessing a certain site.

Open Discussion

11. A serious issue with the conduction of R&D, is obtaining test data sets and comparing them to earlier test sets. Additionally, legislation on collecting data can be very strict in certain countries. These laws make it difficult to obtain the test data sets required to address the type of issues talked about by the panellists. It is, therefore, necessary to clear legal issues before finally addressing the technical issues. This is where cross-border cooperation becomes necessary.
Intel has a voluntary scheme where they do allow the use of their work and home I.P.s in order to collect data about information flows between the different Intel offices.

There is a lack of an international response regarding CERTs. The challenge is for companies to coordinate responses and fixes. On the issue related to some of the work undertaken by the ITU-D Study Group Question 22/1, some of the initial thinking in infrastructure protection networks has historically stemmed from developed free market economies and there is a need to address the issues on a developing countries front.
The work of the ITU-D Study Group 1 Question 22/1 on Securing information and communication networks and best practices for developing a culture of cybersecurity is also another important standard which provides a solid foundation for cybersecurity.
The best way to introduce functionality is through CAPTCHA[1] technology. How does this relate to IP trace back? This is a way to provide for accountability to the source of the message. Cisco has products that make use of these sorts of tools.
The intelligence on information flows is available but it is generally only treated under full non-disclosure agreements. This is certainly one of the main problems with analysing data for R&D purposes.
The US homeland security department has a project which gathers test data sets available for researchers. Those data sets are only available for use within the US. The government has appropriated about 86 billion dollars of data for cybersecurity research of which most is classified.
The infrastructure which runs the internet is largely owned by private companies. This is the main problem when trying to research and collaborate in research and development .

[1] Completely Automated Turing Test to Tell Computers and Humans Apart

The characteristics of the IT industry are only nascent. There is a lot of missing knowledge which does not allow testing for certain threats and anticipation of future vulnerabilities. In this context, liability becomes more difficult in this area than in the car industry for example.
The security issue of the technologies today is due to its development in the 1970s which did not anticipate the complexity and the current use of these technologies today.
There needs to be a roadmap, which contains lessons learned from mature industries which also have extensive legal frameworks in place, which are being exploited right now by the criminal element.

Session 2: Civilian cyber-defence: Is enough being done to raise security IQs and to protect users?

12. Mr. Misha Glenny, Writer and Broadcaster, UK (Author of McMafia, April 2008)
The most secretive organisations are banks. They do not divert the requisite resources for cybersecurity, since they are still in a profit making margin. Once the secrecy is put aside, then it will be easier to collaborate between law enforcement, private industry and the financial sphere.
The real issue about user defects, is that people are very easily manipulated. Hackers employ about 5-10 per cent of their time to creating malicious code and the rest of their time is deployed in social engineering. Hackers have almost entirely discarded the phenomenon of ego-sites.
About 90 per cent of criminal hackers are now after the money. They have linked up with established organised crime groups which fund their activities.

13. Mr. Graham Butler, President and CEO, Bitek Inc - PowerPoint Presentation
About 160 countries do not adopt the same net neutrality attitude that the U.S. has. The money goes into the infrastructure and the telecoms companies. Bitek runs detailed analytical statistics on the networks where it installs its systems.
Secure sites will become hosts to spamming sites since they are able to cover the traffic sent out by the spammers due to their being super nodes. There are approximately 90 encrypted peer to peer solutions going out on the network. Police enforcement is unable to read the information of encrypted networks. In certain countries, organised criminal groups own VoIP networks and it becomes very difficult to stop and shut down such networks because of the unregulated nature of VoIP.
About 78% of people downloading VoIP software believe they can dial emergency service numbers. This is incorrect. This is the reason it is critical to regulate VoIP.

14. Mr. Sean Sullivan, Technical Expert, F-Secure, Helsinki
Education of the end user is important. Cyberthreats are namely a human threat. The internet organises itself and criminals will create a market place for illegitimate activity.
The people that use the technologies will break it themselves so as to up the performance. Should a computer be certified to drive on the information highway like the car needs to be certified to drive on the road? The computer itself is an invaluable resource. People do not realise that it is not only their identity and sensitive information that is at risk, but also their computers which can form part of a *botnet* for example. The end user needs to be empowered to protect themselves. F-Secure helps end users to verify that their computers are up to date.

15. Mr. Ivar Tallo, Senior Programme Officer, UNITAR
It is clear that the best way to ensure cyberpeace is to behave responsibly. Some parts of the dilemma we are facing is the huge influx of new users. Security specialists always say themselves,

it is never enough to behave responsibly. There are hosts of malicious software out there that will seek to break through anyway. Trust in society lowers the cost of transactions and contributes to economic growth. The space of cyberspace has also made us more vulnerable to cyberthreats. This is why we are currently witnessing new types of behaviour which are destabilising the collective online community.
Cyberiots in Estonia last year was a first in the cyberworld. The threat is not on someone's computer but generally on cyberspace which has become part of the critical infrastructure. In a way, the reliance of our everyday life on cyberspace is getting to the point where we have a qualitative jump, where cyberspace becomes part of the critical infrastructure. Therefore, cyberthreats really do threaten our way of life in general, by affecting economic stability. Events in Estonia reflected this context last year. Mass discontent spilled over into cyberspace. First and foremost it was due to civilian discontent in cyberspace.
The GCA tries to define all the relevant actors and that seems to cover it all. However, if we draw a parallel with civilian life in the 'real' world, then this is certainly an angle which will be difficult to control.

16. Ms. Isabella Santa, Senior Expert on Awareness Raising, ENISA
Education is important since most of the security breaches are the result of human errors or human components. Therefore, it is recognised that the human factor is key. Awareness of the risk is the first line of defence in reaching a culture of cybersecurity.
Almost 40% of the initiatives run by ENISA target home users and 30% target small and medium enterprises. ENISA concluded that the situation in Europe is different according to the culture and the knowledge of information security. There is a more developed knowledge in the north of Europe than in the south.
There is a shared responsibility between what the user is doing and what the industry organisation is doing. The question is what the industry is doing in raising awareness within its organisation and how the government is tackling this issue. Collaboration with ISPs is also a key action for raising awareness.

Open Discussion

17. A question was asked about the type of regulatory framework that would work, given the kind of information that could be collected, in order to deal with the issue of civilian cyberdefence.
A debate was undertaken about the certification of computers and the feasibility of such a certification, including costs and potential incentives regarding securing systems. Providing encouragements from ISPs to end users is certainly a possibility; however the feasibility of legislating such certifications remains uncertain.
The internet is not comparable to the car industry or the pharmaceutical industry. These industries remain in a fixed national environment. The internet is not an ordinary phenomenon.
There is an existing basis for international law in WEF authentication procedures for legal documents which binds the receiver and the document on a legal basis.
There are many different regimes which deal differently with VoIP, with some countries banning it completely. This is because they have do not the infrastructure to deal with the traffic flows of VoIP. ITU should possibly lead the approach that carriers and ISPs run through a regulated framework. VoIP has many advantages but if the infrastructure cannot support it, it can be very damaging. The issue comes down to personal identification.

A legal framework is not enough to ensure security in the cyberworld. Education is primary, especially with regards to the continuous evolution of ICTs. Awareness is important and collaboration should be undertaken in this domain.

Session 3: Cyber-attacks: Are we ready for the battlefield of the 21st Century?

18. Mr. Adrian Mc. Cullagh, Professor, Information Security Institute, Australia
Authentication is the main issue in the borderless environment. Jurisdictional issues and cross-border relationships are at the centre of virtual communities. The criminal element is now involved in this in a serious way.

19. Mr. Tom Ilube, CEO, Garlik
The battlefield today is really centred on personal identities. More and more people make decisions about others based on their online profile. Cybercriminals ascribe a lot of value from digital identities. In general, a fraudster exploiting an ID can make about 80,000 GBP on that ID. There are specialisations in harvesting IDs and others which make use of and exploit them. They can be used for immigration purposes such as marriages for visas. Fraudsters reckon they can get the most information about someone online. Real IDs will now be used for 419 scams and other online fraud.

20. Mr. Arkadiy Kremer, Chairman of Russian Association for Networks and Services, Russian Federation and ITU-T SG 17 Vice Chairman Speech
ITU-T SG 17 is the lead study group on telecommunication security. It is responsible for coordination of security across all study groups. One of the new SG 17 initiatives is preparing the annual report for IGF 'Business use of telecommunication security standards'. The report will consist of summary sheets for analyzed standards. The sheets will be prepared by experts mainly from ITU, ISO, ETSI, and IETF so the report will include information about most important ICT security standards.
There are a number of standards in the field of telecommunications and information security. But a standard is the real standard when it is used in real world applications. Business and governmental bodies need to learn more about standards from their business applications rather than from a technical point of view.
By launching this project, ITU will provide leadership on WSIS action line C5, not only in preparing the annual report for IGF on information security standardization processes from the viewpoint of business applications, but also in supporting procurement strategies for developing countries.

21. Mr. Marco Gercke, Lecturer, University of Cologne, Germany
There are many reasons why we are not ready for the battlefield of the 21st century because of the expanse of differences which exist on a cultural, economical, political and developmental level. It is necessary to find a balance. In the criminal law, a balance has been found, but it has taken about a hundred years. Looking back ten years, we realise that a single person can start an attack against millions of computers. This is the result of automation. This is what is lacking in the legal system and is a completely new challenge.
Within these challenges, we need to find a balance and ten years might not have been enough time. It is important to have a look at the situation in developing countries as well, because it is necessary to have all countries on board in order for the solution to be effective.

22. Mr. Cedric Renouard, Co-Founder-Director, Ilion Security S.A., Network Audit by Ethical Hacking, Switzerland
There are two kinds of cyberattacks: the first are indiscriminate attacks with random victims and the second are targeted attacks which are targeting a specific individual, group or organisation. When a small group of highly skilled criminals decide to specifically target a group, the organisation can often find themselves very alone. The war between criminal groups and big companies has already begun. This is an important issue which is often overlooked. If you have a specified target, with the adequate means, the adequate cyberweapons, the adequate skills and the capabilities, then there is certainly a chance that cybersecurity can be overcome.

23. Mr. Anthony Rutkowski, Vice-President, VeriSign - Presentation
A combination of the technology and the platform, including the regulatory framework, can help to provide a secure environment if all the elements come from a trusted source. The trusted service provider identity initiative can help instantly gather information about who the user is dealing with and will be able to quantify the value of the risk. This type of infrastructure is not a solution to everything but will certainly be a valuable security-oriented tool.
ITU-D Study Group 1 Q.22/1 report on best practices for a national approach to cybersecurity: A management framework for organizing national cybersecurity efforts, provides national administrations with a management framework for addressing cybersecurity at the national level and for organizing and implementing a national cybersecurity strategy. As existing national capabilities vary greatly and threats constantly evolve, the report does not provide a prescriptive approach to securing cyberspace. Rather, the framework describes a flexible approach that can assist national administrations to review and improve their existing institutions, policies, and relationships addressing cybersecurity issues.

Open Discussion

24. Licensing is surely a model than can work for verifying ISPs. However, it would be difficult to apply this western world model to developing countries. It is necessary to apply a different range of instruments more suitable for their level of development.
Awareness building and basic education of users is an extremely important element.
Mutual authentication is a theory which should be exploited further. Phishers are now using social engineering techniques with online payment systems for Council. ID management attacks are the new techniques used by phishers in order to collect ID information about people. They attack universities, councils and insurance companies in order to reach the maximum amount of people.
To a large extent, more control of the internet will undoubtedly make it more secure. However, that also means that many websites which might not want to register for security and pay licensing fees might be cut off from the internet. The problem is that security is much more of an issue now than it was 10 years ago.
There has always been a centralised organisation which will facilitate the flow of information and has organised the networks. The internet is an overlay network which redefines how people communicate with each other. It should be within the reach of the developed country to look at the mistakes previously made and to fix their infrastructure accordingly.
Providers will not be able to become part of that infrastructure without the prior authorisation and certification. We are currently at the beginning of the different approaches different groups wish to take in order to tackle the issue of cybersecurity. All of these approaches have something different to offer and we should try to combine them in order to reach an ideal solution. This has

the potential to lead to and reach the exchange of information, ideas and activities from different parts of the world. There is little doubt that the focus is switching to the consumer, which is an easier target for the criminals, rather than targeting banks or other organisations.
There seems to be a consensus that one of the fundamental components of cybersecurity revolves around trust. It is interesting to reflect on that as one of the key needs in the battlefield. It is not as simple in this environment when trust is spoken about. It is about being able to assess an assurance level in a particular context. It is a dynamic environment which is forever changing.

Session 4: Global Challenges require Global Solutions: Are there any in the pipeline?

25. Mr. Sy Goodman, Georgia Institute of Technology, USA
We are going to talk about global solutions which are currently in the pipeline and other solutions which are still in the embryonic stage of discussion.

26. Mr. Stein Schjølberg, Chief Judge, and Chairman of the HLEG of GCA
The secretary general established the Global Cybersecurity Agenda (GCA) in May 2007 and a High-Level Experts Group (HLEG) was appointed in order to advise him on cybersecurity issues. The GCA is an ITU framework for international cooperation aimed at proposing strategies for solutions to enhance confidence and security in the information society. It builds on existing national and regional initiatives to avoid duplication of work and encourage collaboration among all relevant partners.
ITU is the international forum in which actions and responses to promote cybersecurity and tackle cybercrime can be addressed. The HLEG is comprised of experts from governments, industry, relevant regional/international organizations, research institutes, academic institutions and individual experts from every part of the world. The HLEG agreed that the work of the GCA should be focused on the following five work areas:

- Work area 1 "Legal Measures"
- Work area 2 "Technical and Procedural Measures"
- Work area 3 "Organisational Structures"
- Work area 4 "Capacity Building"
- Work area 5 "International Cooperation".

The ultimate aim of the GCA is to make significant progress on the agreed goals in the fight against cybercrime and to increase the level of confidence and security in the information society. It is based on international cooperation, and strives to engage all relevant stakeholders in a concerted effort to build security and confidence in the information society.

27. Ms. Solange Ghernaouti-Helie, Professor, HEC-Université de Lausanne, Switzerland
ICT resources are interconnected and interdependent which is why a global cybersecurity answer is necessary. International cooperation relies upon national levels. Therefore national organisational structures need to be put into place. Awareness is not enough to empower the end user. Concurrently, efficient cost effective security measures also need to be put in place. Resources need to be found at the national level as well. Most of the operational work however must be done at the international level.

28. Mr. Wes Kussmaul, Chairman Authentrus
There are global solutions in the pipeline. Some very good protocols have been available for decades but have not been used.
A potential solution can be based on real estate law. Buildings carry occupancy permits which enable quiet enjoyments. Outdoor rest areas near highways do not enjoy quiet enjoyments. These are exempt from building codes and occupancy permits. However, the highway does its job very well since it permits information flows. If one chooses to be indoors, they get there from the outdoors. Indoors is an alternative to outdoors. PKI represents the first indoor building in the cyberworld. The world PKI stance was ahead of its time. Determining the identity and location of the sender is part of the PKI infrastructure.
However, why should an identity belong to a particular person? Who determines receipt of occupancy permits and who delivers them? State, meaning public authorities, should be the ones determining and issuing certificates. If a digital structure proves to be unsound, the architectural builder could loose their license. Since there is only one issuer of professional licences, then building an unsound structure will cost the builder his licence. www.osmio.org is the website which represents this theory of certification by public authorities.

Open Discussion

29. All kinds of things can go wrong in cyberspace and our increasing dependence on this will make us into hostages eventually. When things go wrong, we won't be able to jump out of the situation because we are collectively hooked on it. We as individuals and organisations are becoming less able to defend ourselves.
It is clear that the ITU needs to play a conceptual role in setting down a roadmap of what each country should be doing in order to secure their cyberspace.

ICAO is a useful analogy for the type of organisational framework or structure which the ITU could envisage looking at in the context of cybersecurity. The ITU-R is already performing many functions which are sought from an international forum envisaged in this domain. The ITU Radiocommunication Sector's (ITU-R) primary objective is to ensure interference-free operations of radiocommunication systems. This is ensured through implementation of the Radio Regulations and Regional Agreements, and the efficient and timely update of these instruments through the processes of the World and Regional Radiocommunication Conferences. Furthermore, radio standardization establishes ´recommendations´ intended to assure the necessary performance and quality in operating radio communication systems. It also seeks ways and means to conserve the spectrum and ensure flexibility for future expansion and new technological developments.

Session 5: Overview of Stakeholder Activities: Who is doing what in Cybersecurity?

30. Ms. Salma Abbasi, Chairman, eWorldwide Group - PowerPoint Presentation: Overview of Cybercrime
The fastest growing usage of the internet comes from the Arab world. Concern over Western morals and principles is high, even though there is economic development in this economy that the internet is providing.

Financial crimes are high on the list of major criminal activity on the internet. Human trafficking and sexual exploitation is an extremely critical issue on the information superhighway which is very troublesome. It is necessary to have sufficient protection against the weakest and most vulnerable users.
Terrorism and radicalisation is another area where the consequences impact us all. Guidance and policies have to come from a neutral organisation. The HLEG work that will come out of this project is therefore vital. It is important that the work done can be implemented. The world needs something other than a report that will sit on the shelf.
Human trafficking is the domain of organised criminal groups. The challenge is to build confidence with each other. Trust plays a central role in helping to alleviate some of these problems. A legal framework needs to be knit into resistant technology to protect organisational frameworks for operation and response and ensure capacity building competences to respond and react and multi-lateral partnerships.

31. Mr. Henrique Faulhaber, Member of the Internet Steering Committee, Brazil - PowerPoint Presentation
The committee is composed of members from government, private sector, civil society and NGOs. The committee's role is to help new CSIRTs to elaborate their activities. The initial CERT was the result of collaboration with Carnegie Mellon University which adapted its training to the Brazilian model.
The Brazil Honeypot Alliance and the SpamPots Project are two initiatives which have been successfully supported and implemented by the committee.
An end user security guide has also been published, in addition to the development of an anti-spam working group in order to ensure continuous education in the domain of capacity building.
The Committee does help other countries in Latin America and certain countries in Angola in setting up CERTs. The Committee is engaged in cooperation with OAS as well.

32. Mr. Jinhyun Cho, Convener of the Security and Prosperity Steering Group, APECTEL - PowerPoint Presentation
APEC has emphasised the importance of securing critical infrastructure after the 9/11 attacks in 2001. The leaders issued a statement on further cooperation in the domain of terrorism and growth. This included setting up 24/7 points of contact and CERTs, including updating the legal framework.
The Ministers sent out a call for action and issued a statement on the security of information and communication infrastructures. The Lima Declaration called for additional action on promoting the development of CSIRTs and for further cooperation between APEC countries.
The APEC has implemented a Cybersecurity Strategy in order to ensure a trusted, secure and sustainable online environment.
APEC implements different items related to cybersecurity mainly through cooperation with other bodies, and through capacity building activities and workshops.

33. Ms. Fredesvinda Insa, Directora de Desarrollo Estratégico de Prueba Electrónica, Cybex, Spain - PowerPoint Presentation
Since 2005, Cybex has been researching with the European Commission on the admissibility of such evidence in court and whether it was being regulated or not in the different jurisdictions in Europe. Cybex is a private firm leading work in the electronic environment and dealing specifically with electronic evidence.

The first question to ask is whether there is an actual definition of what constitutes electronic evidence. The legislative references reveal that there is no specific definition. Generally, by analogy certain definitions are applied from traditional evidence, electronic documents, electronic signatures and means of evidence.
Regarding legislation, there is no specific regulation on electronic evidence in Europe. This makes it difficult to prosecute under these conditions. The question, therefore, is whether it is necessary to elaborate a European framework which would regulate this domain.
A final question to ask is whether there are specific procedures for the obtaining, analysis and presentation of electronic evidence reflected in European legislation. The answer is no. Consequently, European laws adapt themselves by making the analogy with traditional procedures.
Judges and police experts are key actors in this domain and therefore cooperation between these different players is critical.
Should an international legal framework be implemented in the area of electronic evidence and its admissibility in court? This is perhaps a question that a group such as the HLEG can tackle.
Cybex is currently developing a newsletter in electronic format to disseminate best practices within the EU on electronic evidence.

34. Mr. Jean-Charles de Cordes, Head of Cybercrime and Organised Crime Unit, Council of Europe - PowerPoint presentation
A very flexible and pragmatic approach is being funded by Council of Europe and Microsoft, including member states, regarding implementation of the Cybercrime Convention and the Additional Protocol on Xenophobia and Racism.
The main issues being tackled during this approach are:

1. Strengthening cybercrime legislation.
2. Reinforcing the capacities of criminal justice systems around the world in order to better investigate and prosecute cybercrime.

Council of Europe is working closely with many different groups and tries to use its current project to participate in major international events related to cybercrime and cybersecurity. The Council of Europe has created a solid momentum.
In addition to the states which have signed and ratified the Convention, there are also states which have used the convention to improve their legislation and to make it more coherent with the legislation in other countries. This is essentially the basis for international harmonisation in the legislative domain.
The Council of Europe has prepared and adopted a guideline along with industry and law enforcement on the good practices which can apply in all the countries of the world that can help foster the cooperation between law enforcement and internet service providers.

35. Mr. Kenichi Takao, Criminal Intelligence Officer, Financial and High-Tech Crime. Sub-Directorate, Interpol - PowerPoint presentation
I-24/7 communication system is a secure network system linking 124 different countries which allows dissemination of warrants within this network.
NCRP is Interpol's National Central Reference Point for computer related crime. It is an early warning system between IT crime investigation units to provide secure channels for information exchange with minimum delays. Currently there are 120 reference contact points within this system.

Interpol works in 4 official languages, has 24/7 contact points in 81 different countries. Data in NCRP is updated only through informed Interpol channels. NCP exists for operation assistance and for technical investigations.
Interpol's secure website contains a valuable resource of information; the site, however, requires a login and password. This is accessible by end-users after a request is made by Interpol.

Open Discussion

36. The message today is about collaboration. ITU will not take over or replace the different activities and the entities represented. The main issue is to collaborate and agree on an international framework for cooperation.
The executive summary which provides information from everybody dealing with cybersecurity should also provide links to the wealth of information available from all these different sources.
What is the difference between Interpol and Europol? The difference is the area covered by each group. In the field of high-tech crime, Europol has a certain number of high-tech crime specialists while Interpol has a bit less. Interpol, however, collaborates with national police and Europol to support the work undertaken; it does not necessarily take the lead in investigations.
In Japan, anti-spam activities represent important activities for the government. Japan would like to share its experience in security technologies with the rest of the world.
A point was made regarding capacity building and international cooperation. The objectives for these two areas, as part of the GCA, really need to focus on incident response handling. Capacity building is a very important issue and should not be overshadowed by other issues.
Malaysia has agreed to form a strategic partnership with the ITU in order to work together in the fight against cybercrime by setting up relevant activities.
The anti-spam working group was started four years ago and has advanced a lot sine then. More recently, collaboration within the context of a Memorandum of Understanding has been initiated with Taiwan and Japan in order to manage port 25. Most of the spam does not come from Brazil itself but much of it is transmitted through the country as a relay point.
The protocol does consider everyone equally and does not make any differences between races and cultures.
The participants strongly endorse the work done by all three of the ITU sectors:

- Telecommunication Standardization Sector, ITU-T,
- Radiocommunication Sector, ITU-R
- Telecommunication Development Sector, ITU-D.

The delegates strongly emphasized taking into account study group findings, recommendations and reports issued by the three sectors as a sure step forward in securing information and communication technologies.

Session 6: Overview of Stakeholder Activities: Who is doing what in Cybersecurity?

37. Mr. Pierre Ouédraogo, Program Manager, Information Society, Institut de la Francophonie numérique, Organisation internationale de la Francophonie

PowerPoint Presentation
Francophonie is an international organisation whose vision is the freedom of technological choice, namely by educating people about the wide range and availability of technical devices and software.
Sharing is a key word for Francophonie. Free software is seen as a part of digital solidarity and a good opportunity for LDCs to respect fully IPRs. Inclusion of multi-lingual diversity is also very important for Francophonie.
Capacity building through free software is of major importance. Workshops are organised in many African countries. Dissemination of technical knowledge is done through ICT laws and through a network of national free software users.
Networking activities include training to set up human networks, work with national certification agencies, and organising the first African cybersecurity conference which will take place in October of 2008. Prior to the conference, a cybersecurity workshop is being organised in order to prepare for the conference.

38. Mr. Henning Wegener, Chairman, Permanent Monitoring Panel on Information Security, World Federation of Scientists - PowerPoint Presentation
The WFS has formed many working groups called permanent monitoring panels which develop specific projects in order to mitigate planetary emergencies which they then analyse and study in order to reach potential solutions.
The threats emanating from cyberspace are certainly relevant to the correct functioning of many important infrastructures which the world currently relies on. The permanent monitoring panel on cybersecurity was formed in 2001 and is very varied in geographical location and discipline. The technical expertise is focused on the political and institutional aspects of cybersecurity.
The concern with national and international security can be a primary generator for threats which the panel researches in order to find adequate solutions. Among these issues looked at is also the problem of the digital divide.
The use of information weapons is a very real threat for cyberwar. Economic dimensions of cyberattacks and the current emergence of cyberterrorism are of major concerns. Work on international law which would encapsulate cyberwar is an important focus for the WFS. The issue requires examination and interpretation of the UN charters.
The use of ICTs to cause or entail destruction in another country is considered under international armed conflict legal framework. This is an issue being studied in depth by the WFS. The case for a comprehensive international cyberlaw framework is being made by the WFS to the UN in order to harmonise national cyberlaw systems. The ITU could play a determinate role in this domain.
The focus of the digital divide must rely on capacity building and security building. The main point of argument is already reflected in many of the WFS activities. The main goal is to raise awareness in the use of ICTs in developing countries. There should be more action and networking between the networked society and the developing countries as well as other organisations.
Collective efforts are being made to promote a culture of cybersecurity and to create a central information marketplace. The Cybersecurity Gateway could certainly become an important resource for information sharing and resources.

39. Mr. Richard Simpson, Director General, Electronic Commerce Branch, Industry Canada PowerPoint Presentation
A huge internet economy lies at the centre of the information society. Although the growth rate is extremely high, the threats remain ever present. Spam is still around and continues to threaten

network stability and reliability. It has become increasingly sophisticated and dangerous. Threats such as phishing, spyware and botnets are major network threats in their own right.
The real economic costs of these threats are huge. The real cost is an opportunity cost. The internet may not reach its full potential due to all these menaces.
Two interrelated but distinct challenges exist: the internet as an infrastructure and the support of a safe and trustworthy infrastructure. Integrated global approaches are required.
A three-tier cyber defence strategy is essential:

1. Strong technology neutral criminal law
2. Robust domestic and international frameworks
3. Voluntary measures such as private sector codes of conduct

The international response should set the ground rules for the internet economy on a legal, policy and regulatory basis. International instruments are extremely important and certainly play a leading role in harmonisation and finding coherence in the international community.

40. Mr. Manuel Pedrosa de Barros, Director of the Communications Security Office of the Portuguese National Communications Authority (ANACOM), Portugal - PowerPoint Presentation
ANACOM evaluates policies in the telecoms public service concessions by analysing the interdependence between civil protection policies and communications public policies. The focus is to develop a national communications security plan which is a continuation of a study undertaken by the European commission.
ANACOM is developing a plan for the fight against spam by sending out questionnaires to ISPs. It is an adaptation of a questionnaire developed by ENISA last year.
External cooperation is also being undertaken at the national level, the European level and at the international level.

41. Mr. Belhassen Zouari, Head of the Tunisian National Agency for Computer Security (ANSI), Cert-Tcc
The keys to success in a cybersecurity rely on 3 pillars:

1. Technology
2. Methodology
3. Social behaviour

Without these three pillars it is difficult to succeed in ensuring cybersecurity.
Technology tools consist of computer and network tools, data tools, physical security tools and availability and applications. Methodology consists of studying aspects at the managerial level, the legislative level, the operational level and ensuring continuity of services.
The social behavioural pillar concerns cultivating a culture of cybersecurity through continuous actions.
The legislative framework is continuously updated to keep in line with emerging threats and trends in computer crime. The laws on security audit processes are important for ensuring public network security. The NACS certifies auditors which will perform the auditing functions in targeted companies. The auditors are also encouraged to engage in training programs.
Information is collected through collaboration with many different entities such as Microsoft, First, Symantec, Sans, Trend Micro among others.

42. Ms. Bessie Pang, Executive Director, Society for The Policing Of Cyberspace (POLCYB) PowerPoint Presentation

POLCYB goal is to enhance and develop global partnerships. We look at legal issues as well as cyber ethics for children in education for future generations.
Initiatives include international summits, quarterly meetings and other seminars.
POLCYB has a trusted community portal which builds trusted partnerships through a repository of cybercrime related information. The key is sharing information and resources.
Another initiative is the certification for international cybercrime professionals. Skill sets are learned which could be applied to management levels in the field of information security. This includes, for example, the development and management of a cybercrime unit.

Open Discussion

43. A suggestion was made that ITU should host a centre for information exchange and resource for all interested parties to freely access this source, from end users to governments, including private industry.
ITU has two different actions that it is doing in cybersecurity. First, it is the facilitator for C5 and second, it has its own mandate which includes concrete activities, such as, building capacities in different countries.

Session 7: Meeting C5 Goals: How far are we towards meeting the goals of C.5?

44. Mr. Fernando Rivera, Corporate Strategy Division, ITU
PowerPoint Presentation
The question is, how far are we from meeting the goals of C5? The activities are already there, with or without WSIS. WSIS is a framework for cooperation and knowledge sharing. Of course, ITU is not just the facilitator but also one of the main stakeholders.
One way to succeed in achieving our goals is to know where we stand now. Stocktaking is very important. However, if there are no evaluation mechanisms, then it becomes almost useless.
It has been said that ITU is the place where all these initiatives should converge. It has also been said that ITU should not have the monopoly on this either. However, ITU should plan a leading conceptual roadmap to bring actors into a kind of synergy. Therefore, it is proposed to set up a virtual community where all the information can be shared and exchanged, where discussions can take place and where parties from different organisations and countries can meet.
Measuring performance is very important especially in the public, non-profit, academic and commercial environment. But how can performance be effectively measured? Measuring intangible assets (like user awareness) is a challenging task. ENISA has already worked in this domain. It is also important to draw conclusions and propose solutions as a result of these measurement tools.
As a C5 facilitator, ITU needs to measure how it is achieving its goals. Defining a way to assess progress is an important issue. ITU is very well placed to launch a framework which can do this. The GCA is a framework where these measurement tools can be applied for the assessment of current practices and research for potential solutions.
Policy units in government, research and other institutions provide resources and data that can be difficult to quantify. This is why composite indicators, both qualitative and/or quantitative, are necessary to have a common standard from which all data can be measured.
ITU-D has a project to develop a tool which will help to measure cybersecurity.

GCA is a framework which ITU is proposing. Through HLEG and the 5 work areas, GCA can help to aggregate activities in cybersecurity. This will help to collaborate and build some indicators, allowing stakeholders to report on their current activities.
Templates will be developed to help in reporting activities. A web-based platform will also be developed to help discussion and information exchange, as well as, cooperation and collaboration between the numerous stakeholders who wish to participate.
Evaluation of scope through a composite indicator coming from the different stakeholders is necessary. This will only be possible with the cooperation of all the different actors.

Open Discussion

45. The idea is to build the indicators together. The indicators proposed were to give a general idea about measurement mechanisms. This is something that needs to be done with the WSIS community, with necessary comments and feedback from the different stakeholders. All parties need to have the same understanding about what these indicators will look like and the functions they will have.
It is necessary to undertake action now, rather than just have meetings and discussions. The real need for many countries to take concrete steps is critical; especially developing countries which need a structure to help them develop cybersecurity tools.
Additionally, it is requested that all presentations have a similar format and that PowerPoint presentations should be available at least one week beforehand. A summary of the report, including links and the recommendations drawn up by the active debates, should be handed out at the end of the conference and also be made available online.
Finally, the interactive meetings are an excellent way to encourage debate and have discussions between different partners, which will lead to more constructive results.
ITU now has a chance to speak and collaborate with many partners. The announcement of funding of 44 million USD to help bridge the digital divide has been pledged and this brings confidence that things are already underway.
A suggestion was made that the tasks and initiatives proposed during this conference should be made available in a simple website, that would be freely available to anyone wanting to visit it. This would be an initial first step to sharing information about the objectives, the task and the timeframe for Action Line C5, including eventual deliverables.
All actors should be looked to since awareness is the key to building a real culture of cybersecurity: governments, industry, stakeholders, end-users, and academia.
The seriousness of the danger today is quite clear and we should be well prepared. It is a global problem which calls for a global solution and all the parties should work hand-in-hand. The work going on in the GCA and during this C5 event is extremely important.
The participants considered the five work areas of GCA as necessary and appropriate for the work of stakeholders in addressing the challenges faced in Action Line C5. There was also the view that the GCA five areas would facilitate collaboration between various stakeholders because they provide the flexibility for various stakeholders to work in the areas of their competence without the need to categorize the types of stakeholders.
In regard to the work currently being done by stakeholders, it is important to highlight the human factor as well. Although we talk a lot about technology, organised crime is also using the online environment to perpetuate even greater crimes such as human trafficking and forced prostitution.
Will there be a report disseminating the general ideas, visions and discussions which have taken place within ITU in order to share this with groups other than the ones which took part in the conference?

Yes, currently the secretariat does envisage putting out a release ASAP which will be available publicly.
Would it be also possible to have an easier and more open website which would facilitate browsing in order to find the information searched for?
A classification of the information for a future website will be sent out to all the participants in order for them to comment and add their input.
Links are extremely important and it is suggested that as much information about the different participants be circulated as possible. PowerPoint are also excellent reference materials and these should be posted online. May 31, 2008 will be the deadline for sending out all presentations to the secretariat.
A comment was made about the importance of this meeting, as well as the previous HLEG meeting, which were highly informative.

Conclusions and Proposals

Closing Remarks by Deputy Secretary-General, Houlin Zhao

46. I come here to thank you for participating in this event and for the presentations that were given. This meeting has been very fruitful, interesting and useful. This meeting and the HLEG meeting, were both well represented in participation of stakeholders from all different areas and regions, which is a remarkable achievement. There is a converged view that ITU needs to change the format of the cluster event. The agreement reached this morning was that ITU should have more active debate and discussion between panellists and the participants.
These sessions should not be used to exchange information on which organisation is doing what. This discussion is useful, however, it is more important to find out from all sectors about emerging issues and ideas. This would certainly help participants to make better use of their time.
This year, we received around 1400 delegates who accepted the invitation to come to the cluster of WSIS related events. However, only 490 actually attended in person. This is not bad and this particular group was very well attended. This session was extremely active and a very good development regarding interactivity in a session.
We invite all the agencies to consider, with their management, endorsing this proposal for creating a culture of cybersecurity. Open consultation meetings will be set up for interested parties in order to find out what programs can be established and how a collaborative process can be set up.
We really need to look at the way in which we can mobilise society members, take proper action in order to evaluate the work already done and to anticipate working together on future activities.
If any agency wishes to organise conferences in conjunction with these cluster of events, it would certainly be very beneficial to the whole process of collaboration and information sharing.
The UN agencies realise the importance of these activities and they want to see the concrete changes these discussions will bring. If everything is left to ITU, then it will be a long process and this is why the participation of all stakeholders is vital. We really need to find ways to work together with all actors in the information society. This group can certainly be a good example about how all these different stakeholders can work together.
I would like to take this opportunity to thank you for the work put into this session and am very pleased with the result of this group.

UNDP, UNESCO, FAO, UNDESA, UNCTAD & ITU will meet and discuss the results of these meetings, since they are all involved in the WSIS, and talk about the different proposals and recommendations made.
Would there be a possibility for audio casting the meetings next year? Would it be possible also to have remote participation when the floor is opened up for comments?
Yes, the ITU will certainly make these efforts to help disseminate the audio casts and enable remote participation. It is also agreed that translation will also be available next year.
Thanks were expressed to all participants. The meeting was a success because of the active participation of all the stakeholders.

Summary of proposals and recommendations for future actions

47. The Panellists and Speakers debated about what future strategies, solutions, partnerships, frameworks and what focus areas needed to be put into place in order to concretise ITU's role in building confidence and security in the use of ICTs. There was a general view that ITU Global Cybersecurity Agenda was the appropriate framework for multi-stakeholder cooperation in cybersecurity and to concretise the role of ITU in this domain.
A number of specific proposals were made by participants:

1. Ensuring trust through technical solutions:

    - reputation services;
    - trusted identification;
    - cryptography through quantum technology;
    - public key infrastructure namely ITU-T recommendation X.509;
    - multi-model biometrics;
    - guaranteed packet traceback;
    - mutual authentication.

2. Establishing Frameworks in all domains:

    - legal framework reflecting strong technology neutral criminal law;
    - organisational framework for operational activities and response;
    - ITU-D study group one Q.22/1 Report on best practices for a national approach to cybersecurity: A management framework for organizing national cybersecurity efforts;
    - technical framework based on globally accepted security standards and private sector codes of conduct;
    - capacity building competences to respond and react and multi-lateral partnerships;
    - industry framework for multi-lateral partnerships.

3. Awareness-raising through:

    - education of the end-user;
    - elaboration of a roadmap based on the experiences of mature industries;
    - open research of private, public and academic sectors;
    - capacity building activities.

4. Promoting cooperation through:

    - a flexible framework based on the five work areas of the GCA;
    - collaboration between private and public sectors;
    - collaboration between law enforcement, private industry and the financial sphere;
    - finding a balance between the cultural, economical, political and developmental differences of each country in order to enable international cooperation.

5. Nominating a centralised organization like the ITU with a structured framework in the areas of technical measures, organizational structures, capacity building and international cooperation for:

    - facilitation of the flows of information through an organised network;
    - enabling information hosting, sharing and cooperation between all stakeholders through ICTs, such as the ITU cybersecurity gateway;
    - measuring performance, especially in the public, non-profit, academic and commercial environment;
    - creating a roadmap of what each country should be doing in order to secure their cyberspace.
    - dissemination and implementation of recommendations and reports from the three sectors: ITU-D, ITU-R and ITU-T