WSIS FORUM 2016
2-6 May - Geneva

Thematic Workshop

From Cybersecurity to "Cyber" Safety and Security
(EC Medici Framework of Cooperation)

3:00 PM - 4:30 PM, May 5 2016
Room L, ITU Montbrillant

Moderator

Alfredo M. Ronchi *(Secretary General, EC MEDICI Framework, Italy)*

Speakers

Dr. Pavan Duggal *(Head Pavan Duggal Associates – India)*

Dr. Andrea Medico *(Innovation Manager, Intellitronika - Italy)*

Prof. Sarah Fox *(Associate Professor, Coventry University – United Kingdom)*

Prof. Chiara Francalanci *(Associate Professor, Politecnico di Milano - Italy)*

Dr. Matteo Basso *(Technical Secretariat, Observatory on Security and Defence CBRNe – Losanna - CH)*

Dr. Samia Melhem *(Lead Policy Officer, Global ICT Group, Transport & ICT, The Word Bank - USA)*

Prof. Lynn Thiesmeyer *(Full Professor Faculty of Environment and Information Studies, Keio University – Japan)*

Dr. Tin Win Aung *(Chairman of Myanmar Computer Company and President of the Environmental and Economic Research Institute, Yangon - Myanmar)*

Link to WSIS Action Lines

1) The role of governments and all stakeholders in the promotion of ICTs for development - (Safety and security are integral part of human rights - as stated in art 3,22, 25 - The Universal Declaration of Human Rights).

2) Information and communication infrastructure: an essential foundation for an inclusive information society - (Access to public official information, Public access to information, Public domain information)

4) Capacity building (education and training in the field of safety, disasters, emergencies)

5) Building confidence and security in the use of ICTs (extension of the line)

7) ICT applications: benefits in all aspects of life (Disaster recovery, E-agriculture, E-environment, E-health, Sustainable production and consumption)

10) Ethical dimensions the Information Society (Common good, Ethics, Human rights, Preventing abusive uses of ICTs, Values.)

11) International and regional cooperation (Infrastructure development projects, Regional action plan)

Link to SDGs

SDG 2, SDG3, SDG6, SGD6, SDG7, SDG8, SDG9, SDG11, SDG16, SDG17

Outlining the role of ICTs in Safety & Security

Alfredo M. Ronchi

Since its conception and first phase, held in Geneva, WSIS was characterized by its specific focus on "society" and the deep involvement of both stakeholders and civil society in the process: a citizens centred approach.

It was very evident to both technologists and humanists that such a revolution, likely to change significantly not only life but also society, cannot be managed by companies or governments only.

The idea to open the discussion about the impact due to new technologies and their future uses and developments to different actors ranging between governments and civil society it was and still is greatly relevant and extremely positive.

Among the other positive effects, the WSIS outlined both threats and opportunities offered by the ICTs counterbalancing the too often abused trend of blind innovation technology trained.

Nowadays more than fifth teen years later, if our agenda really includes sustainable development goals, a multi-stakeholder multidisciplinary approach is needed in order to approach and positively solve complex problems, how to foresee the effects on society due to new technologies in 20, 50 years or more.

Let us now focus on a specific topic. The action line "C5. Building confidence and security in the use of ICTs", in charge to ITU, addressed some concrete needs in order to make feasible the implementation of the rest of the services (e.g. Government, Business, etc.). Cyber frauds, viruses, cyber identity and spam were, in 2003 - 2005, some of the main obstacles.

Nowadays the demand for "safety & security" in all its forms has increased, especially quantitatively and qualitatively, making clear the need for new approaches to enable the entire sector to ensure better results. It is time to extend the scope from "confidence and security" to a much more general scenario including not only security in a broader sense but even safety, natural and human disasters recovery and management, and more.

Safety and security are integral part of human rights; we must provide all the efforts in order to guarantee such rights (as stated in art 3,22, 25 - The Universal Declaration of Human Rights).

We must promote the opportunity to share experiences and best practices among countries and foster research thanks to the WSIS.

On the occasion of the High Level Policy Statements on May 2015, H.E. Mr Yasuo Sakamoto, Vice-Minister for Policy Coordination, Ministry of Internal Affairs and Communications (Japan), said - on the occasion of natural disasters ICT is the lifeblood to ensure citizen's safety.

Looking from a different perspective: we outline the role of ICTs in risks assessment and management. ICTs are playing key roles in a number of "risky" scenarios from health and children abuse to homeland security and law enforcement, crimes, trafficking (humans, drugs, weapons, artefacts, etc.) and even safety on working places and mobility.

As Mr. Sunil Bahadur Malla, Secretary, Ministry of Information and Communications in Nepal, told us on the same occasion on May 2015 - ICTs were crucial in recovering the territory during and after the recent earthquake.

Internet of things, grids, network of sensors, remote sensing as well as Near Field Communication glued by networking are some of the building blocks of safety and security apps. Of course we cannot forget the need for an international regulatory framework, in a globalised interconnected world we cannot rely on local not harmonised laws and regulations.

In conclusion I would like to stress the positive effects due to the WSIS process and its outcomes, and suggest to include and to promote a wider range of "security" topics under the WSIS umbrella endorsing a holistic approach to the "Safety, Security, Disaster Recovery and Management" sector.

Keywords:

Cyber Safety & Security, CyberSecurity, CyberSafety, Disaster Recovery, Disaster Management, Big Data Analytics, Law Enforcement, Risk Assessment

Short Bio

Alfredo M. Ronchi is the secretary general of the EC MEDICI Framework, founder and chair of the JRC S2D2 Cluster on Safety and Security. He is appointed by ICNM as a member emeritus of Executive Board of Directors of the World Summit Award and member of the board of Global Forum and ENSA. MEDICI's delegate at WSIS since the first phase (Geneva 2003).

He is member WSA Grand Jury and president of eContentAward Italy, coordinator of several international projects, member of the Scientific Committee of Global Forum (F-USA), Sacred World Foundation (New Delhi), Fondazione Nuove Comunicazioni (Italy).

He is appointed as an expert c/o the European Commission, the Council of Europe, the Italian Association of Banks (ABI), National Research Council (CNR). Consultant: IBM (Lugano CH) 1982-83, Team Informatica s.a. (Lugano CH) 1981-83, Thorn/Sylvania/GE Lighting, 1989-94, GE Medical Systems, 1990-93, BolognaFiere 1994-1995, Austrian Ministry of Culture 1999, Ministerium für Wissenschaft, Weiterbildung, Forschung und Kultur des Landes Rheinland-Pfalz (2000-02), Norwegian Ministry of culture – Riksantikvaren, Municipality of Christiansand, Italian Association of Banks (ABI),

Author of more that 350 papers, author/contributor of books: eCulture, eGovernment, eHealth, eLearning, eCitizens. Mr. Ronchi is a professor at Politecnico di Milano (Engineering Faculty).

Alfredo M. Ronchi
EC MEDICI Framework
Email alfredo.ronchi@polimi.it

Cyberlaw , cybercrime and cybersecurity

Pavan Duggal

Cyberlaw as a discipline has evolved substantially ever since its early days but needs to develop proactively and by leaps and bounce.

The International Conference on Cyberlaw, Cybercrime & Cybersecurity organized by Cyberlaws.Net and Pavan Duggal Associates has been contributing to the evolving jurisprudence on Cyberlaw , cybercrime and cybersecurity.

There is a need for the world to start addressing legal issues pertaining to cyber security and Internet jurisdiction in a holistic manner.

With Cyber terror now an increasingly significant vector, cyber terrorism needs to be effectively addressed.

Given the reality of mobile web, Mobile Law needs to substantially develop to enhance the frontiers of Cyberlaw jurisprudence to facilitate seamless mobile based payments, m-banking, mobile commerce and mobile paradigm as a whole.

Consequently, Cyberlaw needs to acknowledge, declare and recognize the right to access the Internet as part of universal human rights.

Given my work in Cyberlaw jurisprudence, I believe that Cyberlaw needs to tighten its belt in terms of dealing with emerging legal, policy and regulatory challenges thrown up by newly emerging areas of technology, whether it is the Internet of Things, 3-D printing, robotics, nano-technology , drone regulation, social media, Over The Top applications, digital and virtual currencies.

Today, darknet has appeared presenting cybercrime as a service and as an economy. Legal frameworks need to be established to regulate Darknet and prevent its misuse for cyber criminal and other related purposes.

WSIS Forum 2015: Policy Statements

It is recommended that an appropriate International Convention on Cyberlaw & Cybersecurity should be drawn up.

This should not be highly complex containing highly complicated statements, instead it should consist of universally accepted principles and norms which have been accepted across the world and which can inform the respective national policies in Cyberlaw and Cybersecurity.

The said International Convention on Cyberlaw & Cybersecurity needs to be broad, generic and engulf within its own self, broad universally accepted parameters and minimum common agreed demoninator principles and building blocks impacting Cyberlaw and Cybersecurity.

The WSIS Forum 2015 workshop on Cyberlaw An Asian Perspective has unanimously recommended about the need for such an International Convention. The said workshop has recommended that ITU initiates a working group for the purposes of determining the scope of issues and focus areas to be covered in the said International Convention on Cyberlaw & Cybersecurity.

The International Convention on Cyberlaw & Cybersecurity is an impending need of the times, would indeed be path-breaking and would immensely help to clarify the evolving jurisprudence pertaining to Cyberlaw & Cybersecurity.

This is yet another wonderful golden opportunity for ITU to seize thought leadership and contribute to an evolving Cyberlaw jurisprudence.

There is a need for complete harmonization of divergent cyber legal frameworks in different countries to promote the further proliferation of Internet.

Lot of work and development in cyber legal jurisprudence has to take place in the next coming five to 10 years. This work cannot be done alone. All stakeholders need to contribute in this humungous exercise. On the occasion of the ITU WSIS Forum 2015, I encourage ITU to contribute to evolving Cyberlaw jurisprudence and take initial initiative in terms of establishing the working group on International Convention on Cybercrime and Cyber Security.

Keywords:

Cyberlaw , cybercrime and cybersecurity

Short Bio

Pavan Duggal, is the Founder & Chairman of International Commission on Cyber Security Law.

Pavan Duggal who is the President of Cyberlaws.Net, has been working in the pioneering area of Cyber Law, Cyber Security Law & Mobile Law. While a practicing Advocate, Supreme Court of India, Pavan Duggal has made an immense impact with an international reputation as an Expert and Authority on Cyber Law, Cyber Security Law and E-commerce law.

Pavan Duggal has been acknowledged as one of the top 4 Cyber Lawyers around the world. WDD [World Domain Day] recognises Pavan Duggal as one of the top 10 Cyber Lawyers

around the world.

His empanelment as a consultant to UNCTAD and UNESCAP on Cyber Law and Cyber Crime respectively, membership of the AFACT Legal Working Group of the UN / CEFAT, consulting as an expert with the Council Of Europe on Cyber Crime, inclusion in the Board of Experts of European Commission's Dr. E-commerce and his work as an expert authority on a Cyber Law primer for E-ASEAN Task Force and as a reviewer for Asian Development Bank speaks volumes of his worldwide acceptance as an authority. Pavan is the President of Cyberlaw Asia, Asia's pioneering organization committed to the passing of dynamic cyber laws in the Asian continent. Pavan is also a member of the WIPO Arbitration and Mediation Center Panel of Neutrals.

As an internationally renowned Cyber law and Cyber security subject expert, at the world stage during the High-Level Policy Statement delivered by him at the World Summit on Information Society (WSIS) organized by the International Telecommunications Union (ITU), UNESCO, UNCTAD & UNDP in Geneva, Switzerland from 25th May – 29th May, 2015 Pavan Duggal has recommended the need for coming up with an #International #Convention on #Cyberlaw & #Cyber Security.

As a thought leader, Pavan has suggested that India requires a new legislation, that is wholly dedicated to cyber security.

Pavan has been the Member of the Public Interest Registry's.Org Advisory Council. He is a member of ICT policy and governance working group of the UNICT taskforce. He is the legal and policy Consultant to Internet Mark 2 Project, which is examining the next level of internet. He has been invited to be an Associated Fellow of the Centre for Asia Pacific Technology Law and Policy (CAPTEL) at Singapore. Pavan is a Member of Panel of Arbitrators of the Regional Centre for Arbitration, Kuala Lumpur and Asian Domain Names Dispute Resolution Centre at Hong Kong.

Pavan Duggal is a Panel Member Of Permanent Monitoring Panel For Information Security- World Federation Of Scientists.

He has been associated with the Ministry Of Communication and Information Technology, Government of India on Cyber Law and Electronic Governance legal issues. He is a member of Advisory Committee on e-governance in

Karnataka constituted by the Government of Karnataka. Pavan is a member of Information Forensic Working Group on E-Information Systems, Security and Audit Association.

Pavan is a member of Multi – Stakeholder Steering Group of the Asia Pacific Region Internet Governance Forum (APRIGF)

Pavan heads his niche law firm Pavan Duggal Associates, which has practice areas, amongst others, in Cyber Law, Business Process Outsourcing Law, Intellectual Property Rights and Information Technology Law, Information Security Law, Defence, Biotech and Corporate Law.

While he has been a member of the Nominating Committee, Membership Advisory Committee and Membership Implementation Task Force of ICANN, Pavan is also the President of Cyberlaws.Net, which is Internet's first ever-unique Cyber Law consultancy.

In addition to that, he is also the founder of the Cyber Law Association and is also the Founder- President, Cyberlaw India.

Some outstanding pioneering work in the field of BPO legal issues has resulted in his being a member of the BPO Steering Committee of ASSOCHAM. Today, he advises a number of BPO concerns on different legal issues relating to outsourcing. Pavan was the Chairman of the Cyber Law Committee of ASSOCHAM and works closely with CII and FICCI.

Pavan is a regular on the lecture circuit. He has spoken at over 1200 Conferences, Seminars and Workshops in the last seven years, and has lectured extensively in select Law Colleges. As a Writer, he has made his mark with 75 Books on various aspects of the law in the last 15 years. He has contributed a continuing weekly column on diverse aspects of the law, titled 'Brief Cases' to the Economic Times, for the last seven years.

More about Pavan Duggal : http://www.linkedin.com/in/pavanduggal.

Pavan Duggal
President, Cyberlaws.Net, Chairman, International Commission on Cyber Security Law
Advocate, Supreme Court of India

Virgo

Andrea Medico

Virgo is the definitive device for the safety of the operators working on highly risked areas.

Specifically designed to meet the Italian Fire Fighters requirement, Virgo is a stand-alone system for the location and positioning of the men in areas where there is little to nothing possibility of visibility. Completed both with a light and acoustic alarm, Virgo can stand extremely high temperature and can work both as a simple location alarm solution and as a system connected to the control room, able to geo-locate the operators and connect them in a rescue team functionality. The main alarms are, air temperature, body temperature, change of position, man down and speed change.

Keywords:

Virgo, Fire-fighters, geo-location inside buildings, safety, connectivity, alarm, rescue, device, life

Odino

Andrea Medico

Odino is the territorial control solution for the Carabinieri in Italy. The COTS device based solution has granted a significant increase in the number of citizens controlled and checked over a single work shift granting an impressive level of efficiency and a total coordination between the police forces of Italy with a first level of common intelligence shared. Its main functionalities are: geolocation, alarm, video/audio streaming in near real time, multiple international database access in real time from the field, coordination, encrypted messaging, ANPR and multiple forces connection. The solution has been studied to be used in several operational environment, both in car, pedestrian, and on motorcycle. ODINO can be connected to external sensors (including third party solution) such as, gun, t-shirt, holster, Virgo, Drones, physical document reading, etc.

Keywords

ODINO, law enforcement, geolocation, multiple database access, sensors, alarm, encrypted messaging, navigation, G-Code

Short Bio

Andrea Medico, born in Rome in 1974 has a degree in Business Administration.

Has been studying and working abroad for several major TLC company dealing with the interconnection sector and being a company representative for the BARG of the GSMA.

In 1998 was the founder and co-owner of Mirafan a consulting company for the definition and introduction of innovative products in the Military and Law Enforcement Sector in the Italian market.

In 2010 Andrea Medico was in the founders group of people that created Intellitronika the first software hose with the specific mission of innovating the security and safety of the people serving and protecting the Italian citizens.

IN 2015 the company decided to go international and is following the path of innovation started in the Italian market, in the challenging international market, bringing to the market new ideas and a different approach to problematics which can now be solved, thanks to the professional team of engineers brought into Intellitronika from its beginning.

Dr. Andrea Medico
Innovation Manager, Intellitronika srl
viale Asia 3, 00144, Italy, ph. +39 065004488,
email: andrea.medico@intellitronika.com

Flying challenges for the future: Aviation resilience in the face of cyber-terrorism

Sarah Jane Fox

The UN Sustainable Development Goals relates to a vision for humanity as well as a social contract between the people of the world. And, whilst sustainability remains the cross cutting focus, the aspect of mobilisation of resources and technology is viewed as a critical aspect in realising development and ultimately pursuing the goals. The overall aim is to 'banish a whole host of social ills by 2030.' However, as old challenges are addressed, new ones ultimately develop and become the fresh nemesis to be tackled.

Transport has always been, and will continue to be, a means to serve to eradicate world inequalities bringing relief and salvation across the globe and no transport mode more so perhaps than aviation. However, aviation has served as both the salvation and the aggressor, having also itself been the victim of terrorist attacks.

Arguably (to date) in 2016, the world could consider itself fortunate not to have witnessed a devastating cyber-terrorist attack on an aircraft. Certainly concerns were raised after the disappearance of MH370 in terms of cockpit tampering; and yet, these reports only touched upon the surface of an effervescing iceberg – set to erupt into a tsunami of devastation. The question inevitably remains 'when' rather than 'if' this will occur.

This presentation reviews the vulnerability of air travel and the preparedness of the industry in terms of coordination (prevention and protection) from the perspective of policy, legislation and organisation.

Keywords:

Aviation; cyber-terrorism; coordination; policy/legislation

Short Bio

Sarah was awarded a Fulbright-Lloyds of London, Law Research Scholarship in 2015/16, and took up a post as a visiting Professor at DePaul University, IALI, Chicago. Her research focuses on EU and International law, strategy, international relations and policy conflicts. Sarah specialises in the field of transport law/policy (particularly aviation) and adjacent measures such as security, safety, infrastructure, organisations/governance. Sarah holds a Ph.D. and Masters degree in EU law (with comparison law analysis – regional and

international). Sarah is also a Fellow (law) of the University of Liverpool and supports the Law (PG) Programmes at the University of Liverpool, UK, whilst also undertaking a role in risk management for the IRM).

Dr Sarah Jane Fox
Associate Professor/Fulbright visiting professor
dr.sjfox@hotmail.com / sarah.fox@coventry.ac.uk
Tel. 0044 2081335793 Coventry University, Priory Street, Coventry UK.

Big Data Advanced Analytics

Chiara Francalanci

Social media represent fast and effective communication channels. On social media, people share their interests and opinions spontaneously, and tend to recreate the network of relationships that they have offline. This unsolicited expression of personal views and open display of connections can provide important knowledge on the behaviour and social role of individuals. Social media analytics are widely used to gather, process and analyse this type information, with broad application in a number of different fields. For example, in crisis management, social media are recognized as the most important communication channel among the individuals involved in a crisis situation and social media analytics can be used to gather first-hand information, to outsource tasks to the crowd, to uncover potential panic situations, and to handle spamming and cheating. In marketing, social media information is commonly analysed to describe individual preferences and, thus, support market segmentation. In human resource management, social media analytics are effectively used to assess the soft skills of people, including important personality traits such as leadership, cooperativeness, and amiability. Regarding security, the opportunities mentioned above are maximized if users are registered and their online identity is known across different social media. While in other contexts this is not possible, when security is the goal pre-registration seems a viable solution and would enable the analysis of social media information to trace user behaviour and identify behavioural patterns that are correlated with specific security threats. Previous experience in these fields shows that social media are a valid complement to more traditional sources of information, with a social role and an ability to improve the safety, security and general performance of a variety of processes.

Keywords

Data science, social media, security, big data, data analysis

Short Bio

Chiara Francalanci is associate professor of information systems at Politecnico di Milano. She has a master's degree in Electronic Engineering from Politecnico di Milano, where she has also completed her Ph.D. in Computer Science. As part of her post-doctoral studies, she has worked for two years at the Harvard Business School as a Visiting Researcher. She has authored articles on the economics of information technology and on data science,

consulted in the financial industry, both in Europe and the U.S., is member of the editorial board of the Journal of Information Technology and senior editor of the AIS Transactions on Enterprise Systems.

Prof. Chiara Francalanci
Associate Professor, Politecnico di Milano
Piazza Leonardo da Vinci 32, Milano, Italy
Email chiara.francalanci@polimi.it, Ph. +39 2 23993457)

Analysis and Estimation of Expected Cyber-Attack Scenarios and Consequences

Matteo Basso

The cyberspace is becoming one of the main elements of vulnerability in national security and has led to a critical situation because the system is always more focused on information sharing and on quick communication all over the world than security. The cyberspace is, in fact, the "easier vector" of the information environment, comprising independent networks of different communication and telecommunication infrastructures. Through this vector it is possible to perform a wide range of cyber-attacks, causing possibly huge negative effects on systems and assets; however, these attacks do not cause human loss or physical damages to the society. In order to protect from this danger, it is necessary to understand and analyze how many and which are the risks as well as the possible actions needed to minimize the consequences of a dangerous event.

Keywords

Safety, Security, Cyber Security, Emergency Management, Crisis Management, Business Continuity

Short Bio

Matteo Basso got a Degree on Economics at University of Verona in 1998 and a master Degree on "Systems and Electronic Technologies for Security, Defense and Intelligence at University Tor Vergata in Roma, Electronic Engineering Department. Working several years for multinational companies, he's an expert on Crisis & Emergency Management, Business Continuity and Health & Safety and he's been working at several projects related to Safety & Security. He's member of Osdife, Observatory on Security and CBRNe Defense, since to 2009.

Dr. Matteo Basso
Via del Politecnico, 1, 00133, Roma (Italy)
Ph. +39 06 72597278, Ph. + 41 766469658
m.basso@osdife.org, info@osdife.org

ICTs for Transform and Innovate

Samia Melhem

Keywords

Innovation, affordability, cyber-security, open data, interoperability

Short Bio

Samia Melhem is an international development expert at the World Bank Group with formal training in management, international finance, computer sciences and engineering. Within the WBG organization, she is located in the Global Practice in charge of Transport and Information Communication Technologies (ICT). Samia leads the Digital Development Community of Practice, and the Knowledge, Learning and Partnerships programs focusing on global capacity building in Digital Development for policy makers and private sector. Her current operational responsibilities include investment operations management, advisory services, capacity building and leading the digital development partnership. Samia has led investment projects in National ICT strategies, Telecoms/Broadband policy, and Private participation in infrastructure, cybersecurity, digital government, trade facilitation, electronic procurement, identity management and urban development in Rwanda, Philippines, Egypt, Kenya, Tunisia, Morocco, Burkina Faso amongst many others.

Samia held several positions as regional coordinator in different regions such as Africa, Middle East and Europe and Central Asia and has experience in more than 50 countries. She represents her group at ITU, UN, WSIS, donor organization and private sector/academia high-level conventions. She has authored several research, working papers and policy notes on innovation and on technology's impact on growth & development. She holds degrees in Electrical Engineering (BS), Computer Sciences (MS) and Finance (MBA)

World Bank, Transport & ICT Global Practice
Samia Melhem
Lead ICT Specialist,
Transport and ICT GP, WB Group

Capture and Readiness of Slow-onset Disaster Information in Southeast Asia

Lynn Thiesmeyer

This research comes from 20 years of localized site research and data capture in slow-onset disaster-impacted communities in Laos, Thailand and Myanmar. Their remote and destitute communities have very little access to IT or other means of communication with the outside, yet they have the highest vulnerability and need the quickest response. And because the economic and ecological effects of slow-onset disasters are less-known, they are less-reflected in country-level data and response, making it more difficult to access timely and practical remedies from international, national, or community-based initiatives.

Slow-onset disasters include deep poverty, the almost total lack of educational facilities and electricity, and the environmental degradation from deforestation, mountain flattening, and overuse of agricultural chemicals that lead to desertification, warming, and widespread drought. Although rapid disasters tend to attract immediate response, their root causes in slow-onset disasters have not gone away. Rather, they now affect larger transboundary populations, increasing their remoteness from communication, their vulnerability, and the threat of more severe disasters. Further, large-scale and rapid-onset disaster responses tend to be generic, providing the same food, water and temporary shelter in all climates and local situations. Yet there are both strengths and needs in local communities that make such responses either redundant or unhelpful.

However, on-site assessments with the use of combined media have been shown to help in providing knowledge of and responses to communities in slow-onset situations by serving as an interface among the local, national, and international stakeholders. We have used rapid assessments with interdisciplinary teams of local and international researchers, with follow-ups over a longitudinal period of at least 5 years, accompanied by fully localized explanations and pinpointed with online mapping. Slow-onset disasters may thus be shown in scientific detail and in a timely manner, before erupting into large-scale disasters. Communities suffering more urgent disasters can also be located and their needs shown in near-real time.

Keywords

Southeast Asia, Slow-onset Disasters, Longitudinal, Localized, Non-IT Interface

Brief Biography

Dr. Lynn Thiesmeyer (Ph.D. Princeton University, 1980), Professor, specialises in Southeast Asian rural development. She is Professor of Environmental Information at Keio University, has been a Research Advisor to the Mekong Institute, Thailand, and is Vice-President of the Environmental and Economic Research Institute of Myanmar. She has organized and moderated multi-nation videoconferences on Asia-Pacific development policy issues for the World Bank and the United Nations. Her publications include Informal and Illegal Movement in the Upper Greater Mekong Subregion (2010), Human Insecurity in East Asia (ed., 2009), and articles on the Millenium Development Goals, landlessness, environmental policy in ASEAN, and China's transboundary water management.

Dr. Lynn Thiesmeyer, Professor
Faculty of Environmental Information, Keio University, Japan 252-0882
Vice-President, Environmental and Economic Research Institute, Myanmar
Tel. (Japan) +81-466-49- 3540   Email: lynnthiesmeyer@gmail.com

Mr. Tin Win Aung
Chairman of Myanmar Computer Company,
President of the Environmental and Economic Research Institute
Yangon – Myanmar