



Thematic Workshop

ICTs for Safety, Security and Disaster Recovery

(EC Medici Framework of Cooperation)

11:00 – 13:00, 12 June 2017

Room A, ITU Montbrillant



Information and
Knowledge Societies for
Sustainable Development Goals
www.wsis.org



World Summit
on the Information Society
Turning targets into action
Geneva 2003 | Tunis 2005 | New York 2015



ICTs 4 Safety & Security



- The aim of the workshop is to provide an overview on the wide range of ICTs playing a key role in the field of safety, security, disaster recovery and more.
- 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.
- An interdisciplinary approach is required in order to solve very complex problems due to the cyber-age. WSIS will act as a global reference point for all those working in these sectors and those who may take advantage from their outcomes.
- A panel of experts coming from different countries and continents will debate on these topics starting from a selection of concrete case study.



Information and
Knowledge Societies for
Sustainable Development Goals
www.wsis.org



World Summit
on the Information Society
Turning targets into action
Geneva 2003 | Tunis 2005 | New York 2015





Speakers



Moderator

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

Speakers / panellists

- Dr. Mahdi Bina (Chief Tehcnology Officer - Presidantial Office – Islamic Republic of Iran)
- Prof. Simone Colombo (Delegate JRC S2D2 Fondazione Politecnico di Milano – Italy)
- Dr. Pavan Duggal (Head Pavan Duggal Associates – India)
- Dr. Jabu Mtsweni (Research Group Leader for Cyber Defence at the Council for Industrial and Scientific Research (CSIR) – South Africa)
- Prof. Sarah Fox (Professor, DePaul University, US – Middlesex University, United Kingdom)
- Dr. Gianluca Sensidoni (Intelligence & Defense Sales Manager - R&D Security Manager - Expert System S.p.A. – Italy)
- Prof. Lynn Thiesmeyer (Full Professor Faculty of Environment and Information Studies, Keio University – Japan)



Information and
Knowledge Societies for
Sustainable Development Goals
www.wsis.org



World Summit
on the Information Society
Turning targets into action
Geneva 2003 | Tunis 2005 | New York 2013



Dr Mahdi Bina
Chief Technology Officer - Presidential Office
Islamic Republic of Iran



Information and
Knowledge Societies for
Sustainable Development Goals
www.wsis.org



World Summit
on the Information Society
Turning targets into action
Geneva 2003 | Tunis 2005 | New York 2013





Risk Analysis and Management

Prof. Simone Colombo

Delegate JRC S2D2 Fondazione Politecnico
di Milano – Italy



Information and
Knowledge Societies for
Sustainable Development Goals
www.wsis.org



World Summit
on the Information Society
Turning targets into action
Geneva 2003 | Tunis 2005 | New York 2013



Cyberlaw , cybercrime and cybersecurity

Dr Pavan Duggal

Head Pavan Duggal Associates – India



Information and
Knowledge Societies for
Sustainable Development Goals
www.wsis.org



World Summit
on the Information Society
Turning targets into action
Geneva 2003 | Tunis 2005 | New York 2013






Integrated Capability Management for Improved Cyber Safety and Security

Dr Jabu Mtsweni
Research Group Leader for Cyber Defence at the Council for
Industrial and Scientific Research (CSIR)- South Africa












HACKED OFF by the drive for autonomy.....

Prof. Sarah Jane Fox
(DePaul University – USA)



Middlesex
University
London
UK










This presentation





Modern day challenges.....
Keeping pace with technology
Connectivity and Movement

Lessons learnt.....

- Technological - advancements /achievements
- Associated (linked) Risks (vulnerabilities)
- Security breaches and unlawful interference

Mechanisms/approaches:

- Pursue - Prevent
- Prevent - Protect
- Protect - Pursue
- Prepare - Respond

Frameworks – Laws, Policies and Agreements
Achieving equilibrium.....
Acceptance and governance






Information and Knowledge Societies for Sustainable Development Goals
www.wsis.org



World Summit on the Information Society
Turning targets into action
Geneva 2003 | Tunis 2005 | New York 2013



United Nations
Educational, Scientific and Cultural Organization



UNITED NATIONS
UNCTAD



UNDP



PARADOX, IRONY & CONFLICTS



International Perspective: key assertions

Human Rights: UDHR (1948)
Preamble: 'Whereas MS's have pledged themselves to achieve, in **cooperation** with the UN...'

Art. 3 'Everyone has the right to life, liberty and **security** of person'

Art. 22 '... as a member of society, has the right to social security and is entitled to realization, **through national effort and international cooperation** and in accordance with the organization and resources of each State....

SDG'S: 'social contract' between the people of the world: ICT accelerates achievements

INTRINSIC LINKS (entitlements + enablers)

Security - Cooperation – **ICT – (Connectivity - Transport) – ICT** – Cooperation - Security

Challenge: **Security and the impact upon fundamental freedoms**



Information and Knowledge Societies for Sustainable Development Goals
www.wsis.org



World Summit on the Information Society
Turning targets into action
Geneva 2003 | Tunis 2005 | New York 2013



United Nations
Educational, Scientific and Cultural Organization



UNITED NATIONS
UNCTAD



UNDP





ICT – An ever connected world

*"Information Superhighway (will) allow us to **share** information, to **connect**, and to **communicate** as a **global community**" (Al Gore, 1994)*

"Extending the world of transport through cyberspace..." (Fox, 2017)

With transport now increasingly also reliant upon ICT





GOVERNANCE: A '5XC' approach

ICT/Transport: Have shared synergies/challenges
Critical national and international infrastructures
 e.g. RISKS... to ICT..... LINKS to Transport.... (vice versa)



Information and Communication Infrastructure (AL C2)

Building Confidence and Security in the use of ICTs (AL C5)

Enabling Environment (AL C6)

Shared physical synergies - lack of policy interaction

KEY: Sharing - ICT pinnacle role - CONNECT: *Communicate: 'Cooperate, Coordinate and Comply.....'*





Frameworks & Governance



"The 1990's also saw fortification of the need for a cooperative worldwide approach through the adoption of Resolution A/RES/49/60 at the 84th Plenary meeting. Within it, reinforcement was given to need to address, '**criminal acts intended or calculated to provoke a state of terror in the general public**'
9 December 1994.

The Resolution, in essence, highlighted that the international community was [fragmented] in terms of a harmonised approach and that there were a number of individual Conventions with different signatories. Highlighted also was the number of attacks **against transport modes**, which was clearly becoming a 'problem.'

1994: the General Assembly, at its 49th session, adopted resolution 49/158 (23 December 1994): UN Manual on the Prevention and Control of Computer-related Crime.

'open borders and revolutions in technology have spread the message and the gifts of freedom, but have also given new opportunities to freedom's enemies... we must be ready...ready if our adversaries try to use computers to disable power grids, banking, communications and transportation networks...' (Clinton, 1999)."

Fox, S. J. (2016) Flying challenges for the future: Aviation preparedness – in the face of cyber-terrorism. Journal of Transportation Security. December 2016, Volume 9, Issue 3, pp. 191-218.



Information and
Knowledge Societies for
Sustainable Development Goals
www.wsis.org



World Summit
on the Information Society
Turning targets into action
Geneva 2003 | Tunis 2005 | New York 2015



FUNCTIONAL LOGIC OF INTEGRATION Past Experiences



US 2001 attack – post 9/11 review suggested the need for strong institutions that overcome **national** and **organisational silos** that prevent inefficient coordination – led to Department for Homeland Security

Findings: Fragmentation makes us vulnerable (internally and externally)

The Soufan Group state that: The Paris attacks of November 2015 and Brussels 2016 shows the **painful costs of technical, institutional and political fragmentation**.

Findings: Better transmission (sharing) of information both nationally and across borders may have prevented both.

In the aftermath: crime fighting - '**more coordination across all stages of investigations, law enforcement and criminal proceedings...**' is needed (which requires ICT use to facilitate the sharing of data)

- Pursue - Prevent

- Prevent - Protect

- Protect - Pursue

- Prepare - Respond



Information and
Knowledge Societies for
Sustainable Development Goals
www.wsis.org

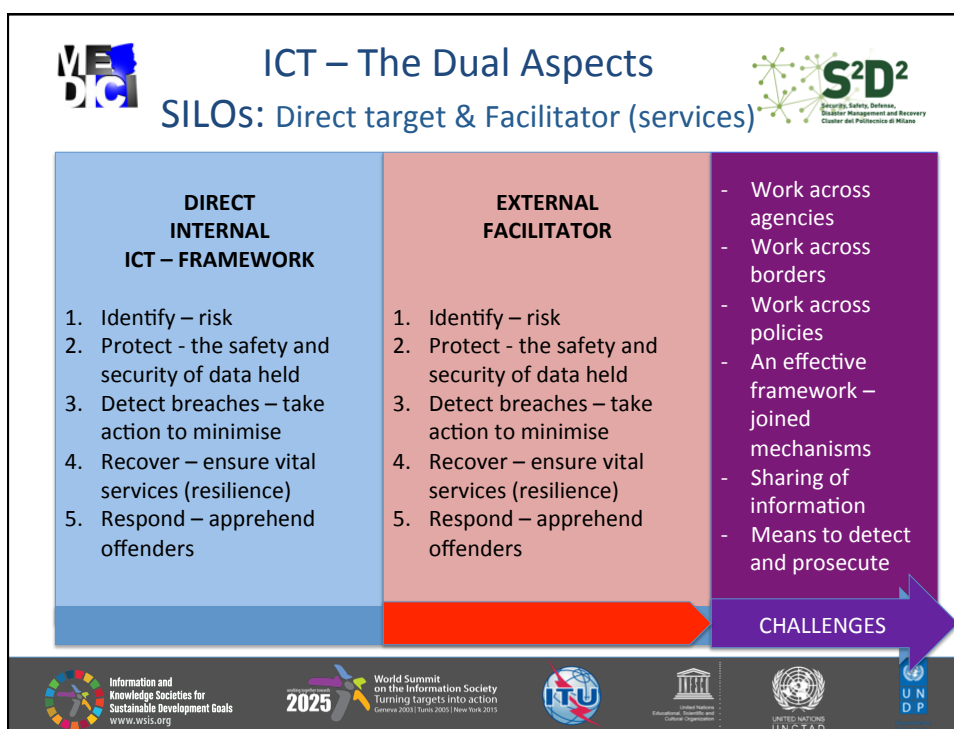


World Summit
on the Information Society
Turning targets into action
Geneva 2003 | Tunis 2005 | New York 2015



ITU CYBERSECURITY STRATEGY GUIDE	Top Government Cybersecurity Accountability Top government leaders are accountable for devising a national strategy and fostering local, national and global cross-sector cooperation.
	National Cybersecurity Coordinator An office or individual oversees cybersecurity activities across the country.
	National Cybersecurity Focal Point A multi-agency body serves as a focal point for all activities dealing with the protection of a nation's cyberspace against all types of cyber threats.
	Legal Measures Typically, a country reviews and, if necessary, drafts new criminal law, procedures, and policy to deter, respond to and prosecute cybercrime.
	National Cybersecurity Framework Countries typically adopt a Framework that defines minimum or mandatory security requirements on issues such as risk management and compliance.
	Computer Incident Response Team (CIRT) A strategy-led programme contains incident management capabilities with national responsibility. The role analyses cyber threat trends, coordinates response and disseminates information to all relevant stakeholders.
	Cybersecurity Awareness and Education A national programme should exist to raise awareness about cyber threats.
	Public-Private Sector Cybersecurity partnership Governments should form meaningful partnership with the private sector.
	Cybersecurity Skills and Training Programme A programme should help train cybersecurity professionals.
	International Cooperation Global cooperation is vital due to the transnational nature of cyber threats.

1	Top Government Cybersecurity Accountability Top government leaders are accountable for devising a national strategy and fostering local, national and global cross-sector cooperation.
2	National Cybersecurity Coordinator An office or individual oversees cybersecurity activities across the country.
3	National Cybersecurity Focal Point A multi-agency body serves as a focal point for all activities dealing with the protection of a nation's cyberspace against all types of cyber threats.
4	Legal Measures Typically, a country reviews and, if necessary, drafts new criminal law, procedures, and policy to deter, respond to and prosecute cybercrime.
5	National Cybersecurity Framework Countries typically adopt a Framework that defines minimum or mandatory security requirements on issues such as risk management and compliance.
6	Computer Incident Response Team (CIRT) A strategy-led programme contains incident management capabilities with national responsibility. The role analyses cyber threat trends, coordinates response and disseminates information to all relevant stakeholders.
7	Cybersecurity Awareness and Education A national programme should exist to raise awareness about cyber threats.
8	Public-Private Sector Cybersecurity partnership Governments should form meaningful partnership with the private sector.
9	Cybersecurity Skills and Training Programme A programme should help train cybersecurity professionals.
10	International Cooperation Global cooperation is vital due to the transnational nature of cyber threats.



PROGRESS?

In the EU – in 2017, the EU Commission:

- will review the EU Cybersecurity Strategy and the mandate of the European Union Agency for Network and Information Security (ENISA), in a bid to align it to the new EU-wide framework on cybersecurity.
- propose additional measures on cybersecurity standards, certification and labelling to make connected objects more cyber secure.

Key objectives and aims remain to:

- (1) increase cybersecurity capabilities and cooperation.
- (2) bring cybersecurity capabilities at the same level of development in all the EU Member States and ensure that exchanges of information and cooperation are efficient, including at cross-border level.
- (3) embed cybersecurity in the future EU policy initiatives from the start, in particular with regard to new technologies and emerging sectors such as connected cars, smart grids etc.

Logos at the bottom: Information and Knowledge Societies for Sustainable Development Goals, 2025, World Summit on the Information Society, ITU, United Nations, UNCTAD, UNDP.



Risk & Security



In the meantime transport remains vulnerable whilst technology becomes increasingly part of today's transport modes and systems:

In June 2011, a University of Texas at Austin research team hacked a Department of Homeland Security drone, bringing it under the control of the students and professor. The team "spoofed" the UAV's GPS signal and took control of the craft.

Connected infrastructure networks such as transport, autonomous vehicles remain vulnerable. The risk of using UAV's in the same way as other transport modes have been used – as a terrorist device, remains a real threat - but, as yet, UAV's are not covered by EU or UN measures in the same way as aircraft-planes are.



FUTURE CHALLENGES.... Digital technologies continue to develop



1. Technical interoperability needs to be aligned to wider frameworks.
2. Frameworks need to cross borders, cross systems.
3. Security and counter terrorism needs to embrace the culture of sharing widely timely and proactively.
4. Lessons from transport need to be embraced by ICT,
5. And, ICT has a role to play in ensuring transport modes are not compromised.
6. Consideration needs to be given to the means to track and bring perpetrators to account for security breaches and terrorist acts.

SPEED IS OF THE ESSENCE

Divisionism remains divisive and dangerous and does not ensure the safety and security of the people of the world





REFERENCES: Link to previous work

Fox, S. J. (2014) 'Safety & security: The influence of 9/11 to the EU Framework.'
Research in Transportation Economics – Special Edition DOI: 10.1016/j.retrec.
2014.07.004 Vol. 45 (2014), pp. 24–33

Fox, S. J. (2015) 'CONTEST'ing Chicago. Origins and Reflections: Lest we forget!
International Journal of Private Law, (2015) Vol. 8, No. 1, pp. 73–98

Sarah Jane Fox, (2016) Flying challenges for the future: Aviation preparedness – in
the face of cyber-terrorism.
Journal of Transportation Security. December 2016, Volume 9, Issue 3, pp. 191-218.

Sarah Jane Fox, (2017) The rise of the drones: Framework and Governance – Why
risk it!
82 J. Air Law & Com. Pp. xx-xx (2017)
(Expected publishing date September 2017)



Information and
Knowledge Societies for
Sustainable Development Goals
www.wsis.org



World Summit
on the Information Society
Turning targets into action
Geneva 2003 | Tunis 2005 | New York 2015



Dr. Gianluca Sensidoni

Intelligence & Defence Sales Manager - R&D
Security Manager - Expert System S.p.A. - Italy



Information and
Knowledge Societies for
Sustainable Development Goals
www.wsis.org



World Summit
on the Information Society
Turning targets into action
Geneva 2003 | Tunis 2005 | New York 2015





Low-tech ICT Measures against Human Insecurity in Border Areas of Southeast Asia

Prof. Lynn Thiesmeyer

Full Professor Faculty of Environment and Information Studies, Keio University – Japan - remote participant



Information and Knowledge Societies for Sustainable Development Goals
www.wsis.org



World Summit on the Information Society
Turning targets into action
Geneva 2003 | Tunis 2005 | New York 2013



Summary



- Dr. Mahdi Bina (Chief Tehcnology Officer - Presidental Office – Islamic Republic of Iran)
- Prof. Simone Colombo (Delegate JRC S2D2 Fondazione Politecnico di Milano – Italy)
- Dr. Pavan Duggal (Head Pavan Duggal Associates – India)
- Dr. Jabu Mtsweni (Research Group Leader for Cyber Defence at the Council for Industrial and Scientific Research (CSIR) – South Africa)
- Prof. Dr Sarah Fox (DePaul University, US – Middlesex University, United Kingdom)
- Dr. Gianluca Sensidoni (Intelligence & Defense Sales Manager - R&D Security Manager - Expert System S.p.A. – Italy)
- Prof. Lynn Thiesmeyer (Full Professor Faculty of Environment and Information Studies, Keio University – Japan)



Information and Knowledge Societies for Sustainable Development Goals
www.wsis.org



World Summit on the Information Society
Turning targets into action
Geneva 2003 | Tunis 2005 | New York 2013





Thank you very much

ICTs for
Safety, Security and Disaster Recovery
(EC Medici Framework of Cooperation)

alfredo.ronchi@polimi.it



Information and
Knowledge Societies for
Sustainable Development Goals
www.wsis.org



World Summit
on the Information Society
Turning targets into action
Geneva 2003, Tunis 2005, New York 2015

