WSIS Forum 2018 OUTCOME DOCUMENT

Template for Submission of Executive Summaries for

Thematic/Country Workshop/ Action Line Facilitation Meetings/ Interactive Sessions/ High Level Dialogues/Publication Releases/Briefings

Deadline: Thursday 22 March, 2018

Exception: For sessions on Friday 23 March, please send at the latest 2 hours after the session

Please note that the WSIS Forum 2018 Outcome Document will be released on the ***23rd of March***

(the last day of the Forum)

1) **Title of your session:** ICTs for Safety & Security: International case study

2) **Name of Organization/s organizing the session:** EC MEDICI Framework of Cooperation

3) **Relevance with the WSIS Action Lines – please specify the Action lines C1 to C11**
   - C1. The role of public governance authorities and all stakeholders in the promotion of ICTs for development
   - C2. Information and communication infrastructure
   - C4. Capacity building
   - C5. Building confidence and security in the use of ICTs
   - C6. Enabling environment
   - C7. ICT Applications: E-government
   - C7. ICT Applications: E-health
   - C7. ICT Applications: E-environment
   - C10. Ethical dimensions of the Information Society
   - C11. International and regional cooperation

4) **Key achievements, announcements, launches, agreements, and commitments (these will be reflected in the press release and Outcomes Document of the WSIS Forum 2018)**
   1) First achievement: further promote 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.), natural and human disasters recovery and management, and even safety on working places and mobility. WSIS may

play a key role in this sector becoming the reference point for all those working in these sectors and those who may take advantage from their outcomes

2) Second achievement: promote a multi-stakeholder forum on social, economic, ethical impact of the Information Society.

5) Main outcomes highlighting the following:

I. Debated Issues

On the occasion of the recent editions of the WSIS Forum MEDICI organised different workshops to showcase on the one side the richness of applications and services provided by ICTs in the field of safety, security and disaster recovery and management and to contribute to provide a reference point for all those working in these sectors and those who may take advantage from their outcomes. This year we continued this path selecting additional international case study both to approach new sectors and enrich the platform of skills and competences involved.

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). In addition, a number of SDGs are tightly connected or rely on safety and security: SDG 2, SDG3, SDG6, SGD6, SDG7, SDG8, SDG9, SDG11, SDG16, SDG17. Some of the specific fields are: food & water security, human security, safety, critical infrastructure resilience, drugs security 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.

Looking from a different perspective: we outline the role of ICTs in risks assessment and management. They 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.

Of course, technology it is not enough to solve problems, it is well known and demonstrated that a holistic, interdisciplinary approach and a culture of "safety &

security" taking adequately into account human factors are the basis in order to obtain good results in this area.

We must promote an interdisciplinary approach and a “culture” of safety & security, they are the basis in order to obtain good results in this area; foster the exchange of experiences and best practices among countries and promote research thanks to the WSIS.

On the occasion of previous editions of the WSIS Forum (e.g. 2014, 2015, 2016) some eminent speakers underlined the key-role played by ICTs on the occasion of natural disasters and other critical events, they said that cyber technologies have fuelled the hope of people affected by the natural disaster. The availability of low price high performance devices and the proactive activity of clever developers have boosted the production of a number of smart solutions spread in different countries all-over the world. Due to the actual “silos” segmenting these sectors it is quite difficult to have a comprehensive vision on these resources and success stories, there is a need for a holistic approach and best practice sharing.

Internet of things, machine learning, grids, network of sensors, remote sensing as well as near field communication and, why not, unmanned vehicles glued by networking are some of the building blocks of safety and security in different fields.

The nine case study presented by the distinguished speakers on the occasion of the ICT for Safety and Security led to the following outcomes: there is a need to improve the visibility of ICT applications devoted to safety and security raising the same level of awareness actually limited to cyber security. The case study presented on the occasion of the workshop this year and the one already presented in the last editions of the WSIS have strengthened this need. Achievements in these fields positively impact the human rights and must be shared among researchers and countries. The WSIS Forum is the key forum for discussing the role of ICTs as a means of implementation of the Sustainable Development Goals, if we consider ICTs as powerful means to implement SDGs we must include and adequately take into account ICTs applied to safety and security in a broad sense, they are relevant part of SDGs as outlined many times both within the UNGA Overall WSIS Review and the UNDP 2030 Agenda for Sustainable Development SDGs.

An additional relevant issue emerged on the occasion of the workshop, as sometimes happens after revolutions, revolutionaries wonder if what they achieved is actually what they were hoping for. The original idea of computer scientists in the “hippies”

counterculture era was aimed to empower citizens and provide them much freedom. Almost fifty years later, after the chimera of the "happy cyber-world", some of us have started thinking that the foreseen Orwellian "1984" has simply come true ten, fifteen years later: globalisation, always on devices, position tracking systems, CRMs and users' profiles, CCTVs and IoT; are those technologies framing citizens? Thoughts for some time have circled around how the speed of the new information revolution renders us less capable develop a critical approach able to foresee the social, ethic, economic impact of such revolution in a long-term perspective. So, in recent times we started facing a wave of criticism about the evolutionary path of the information and knowledge society, for quite a long time ICT gurus and humanists didn't interact too much, the true power of cyber technology was largely unexpressed, there were some alerts as Artificial Intelligence, Virtual Reality, Robots often seen from humanists as potential danger for the mankind, but nothing concrete happened. The turning point was probably the exploitation of the Internet and the dissemination of information. Information is built on top of single or aggregation of data, for quite a long-time people use to think that cyberspace is a "black hole" without memory where you pour data without any side effect. Young generations shared on line sensitive information in order to access a videogame or chat with friends and more recently posted images and clips about their private life; does this mean "goodbye privacy?" As a consequence of a lack of "culture" in the use of emerging technologies now we have to deal with serious problems related to information ownership, use, abuse and misuse, not mentioning cybercrimes. An additional drawback is due to the deep technological intrusion affecting our daily life, we feel framed by cyber devices more than supported.

Some evident outcomes of this feeling are the "right to disconnect" - controversial reform of French labour law by the labour minister Myriam El Khomri back in May 2016 and the "right to obsolescence" or the "right to be forgotten" due to Viktor Mayer-Schönberger, the author of "Delete: The Virtue of Forgetting in the Digital Age". All these to do not mention the cultural, social and economic impacts not always positive especially in a long-term perspective.

Technologies originally conceived by idealists to provide much more freedom and wellness to humans took then a wrong path framing humans due to all the constraints placed upon us with new technologies. For instance, as liberating as they are - by providing flexibility and instant connectivity - we have become enslaved to our devices, fearful of losing out information and access in an increasingly competitive and fast-paced world. Consequently, our bodies have suffered, as have our minds (due to information

overload), what of our work-life balance -- and this is just to begin with! Ranjit Makkuni's paper "Betrayed IT Revolution" and presentation outlines a vision for new design of devices, clutter-free access to web documents to create deeper learning experiences. At the implication level, the project rethinks implications for new design of web mark-up languages that support the creating of 'privacy' based secure browsing.

In conclusion we would like to stress the positive effects due to the WSIS process and its outcomes, panellists suggest to establish in the WSIS framework a global observatory on ICTs for safety, security and disaster recovery and to include and promote a wider range of "security" topics under the WSIS umbrella endorsing a holistic approach to the "Safety, Security, Disaster Recovery and Management" sector.

As a follow-up of the active discussion raised by the "IT betrayed revolution" panellists and some distinguished participants decided to activate a working group to further discuss about this relevant topic identifying the WSIS as the perfect framework to approach the human wellness centred development of the information society. The seeds for such a debate were already present since the 2003 Geneva phase of the WSIS, at that time Ethics and Info-Ethics have been a key discussion topic.

The full set of abstracts of the contributions follows:

Herve Rannou (CityzenData, France): ***Time series and geo time series: a disruptive approach in detecting weak signals in security and cybersecurity.*** Traditional IT architectures are driven by business applications related to relational databases. If it is adapted to transactional applications, it leads to silos of data including formats and semantic that differ depending on the business, application, organisation. Time Series is a disruptive approach in which the key data is not related to the business content but it is just the time and the geo location. Originally designed for sensors and IoT data, Time Series appears is the most performant and efficient way to cross different sources of data and to detect weak signals, anomalies … including predictive analysis, Artificial intelligence for all kind of data according they are timestamped. All major digital companies and now major groups use Time Series database technologies. Geo Time Series is an evolution of Time Series in the case the data can be geo-located. For security and cybersecurity, it becomes an opportunity to cross any kind of data to look for weak signals in the flow of big data: any event on internet access or operation, any event on social network, event related to a mobile phone, travel ticketing, police control …

The today Big Data reproduces the model of silos, Geo Time Series appears as disruptive technology to explore data in a scalable perspective.

Nadia Saad Noori (Teknova, Norway): ***Next Generation ICT and Machine Intelligence enabling safe and secure societies.*** Today, we are witnessing a multifaceted digital revolution with high-performance computing, broadband communication, sensing and artificial intelligence integrated in our daily human life. However, societies in the digital age became more complex and new vulnerabilities emerged with this borderless digital medium. Freedom and connectivity was the bright side of a digital age connecting cyber and physical worlds (e.g. IoT, UAV). Unfortunately, a dark side is hidden away in the corners of the dark web where criminals and terrorist organization exploited such tools for malicious purposes. Recent years have witnessed high-profile security challenges on major occidental cities in e.g. France, UK, Belgium and USA such that law enforcement agencies are confronted to extreme situations. Crime organizations are getting networked with international constellations for a more organized planning and execution of the threats using the newest technologies. In this talk, I will present few results from our research on how these trends will impact towards safe and secure societies by involving smart sensing and machine intelligence. Example applications on surveillance, security and disaster management will be provided for illustration of the impact of this next generation ICT.

Hayley Watson (Trilateral Research, UK): ***ICT for good: Enabling citizen resilience through ICT-based interactions.*** ICT's are almost certainly a powerful tool in building citizens resilience to crises and have certainly contributed to societal changes with regard to their uptake and impact, as the world of crisis informatics has shown. Yet, it is important to go beyond a technological determinist view of ICTs in this realm, to a wider consideration of the organisations, economic and social considerations that impact uptake and therefore their usefulness. This presentation explores how organisational, economic and societal considerations can impact the adoption of tools and their use to build citizens resilience. It concludes by considering next steps in research and development in this field, emphasising the need for co-design practices that engage with ethical, legal and social considerations. Keywords: Social Media, Preparedness, Resilience, ICT, Social Considerations, Ethics & Privacy

Pavan Duggal (Pavan Duggal Associates, India): Legal, Policy & Regulatory Issues concerning ICTs for Safety and Security

Sarah Jane Fox (Middlesex University, UK): ***Policing Society: Utilising "cool gadgets and tools".*** As the WSIS Forum acknowledges, ICT can present solutions to SDG's: "Robots, Drones, Virtual Reality (VR), Applications and Online platforms are more than just "cool gadgets and tools" they can be used to contribute added value to humanity." This paper forms part of on-going research, which explores this concept and the use of such technology in today's civil society. And, whilst the research acknowledges the value of new advancements, the research has as an objective, to explore both the challenges and opportunities presented by the use of such technology; which, whilst, to some may be received with enthusiasm, being perceived as 'cool;' to others, they are viewed as tool that are to be feared and met with trepidation. Therefore, one of the key challenges with advancing technology is to achieve equilibrium between these viewpoints. This particular paper, presented at the WSIS-2018-Forum, relates to the use of drones; wherein, the specific focus is to showcase the positive contribution to humanity when used by the police to assist in their role – which invariably includes:

- protecting life and property;
- preserving order;
- preventing the commission of offences; and,
- bringing offenders to justice.

So, whilst differences of thought of such technological may continue to exist, this presentation provides a unique understanding of the success of such tools. This paper therefore recognises a key goal of MEDICI, which is to promote the use of digital and other advanced and emerging technologies, which aim to support social and economic development, whilst additionally protecting our society – and invariably keeping us safe and secure. KEYWORDS: Drones, Policing, Safety and Security

Alessia Golfetti (DeepBlue, Italy): ***Human Factors for safety and security: case studies and challenges.*** Human Factors is the scientific discipline concerned with the understanding of interactions among humans and other elements of a system. Human

factors experts adopt a systemic approach to understand the interactions among: 1) people who do the job; 2) actions and tasks they perform; 3) resources and technologies necessary to complete the job; and 4) the social, economic and physical environment in which they work. The presentation will outline what it means to use and adopt a Human Factors approach in different safety and security contexts. It will explore the different interactions among humans and other elements of a system by providing concrete examples taken from three European projects in the field of cyber security (Hermeneut - Enterprises intangible Risk Management via Economic models based on simulation of modern cyber-attacks), crowd management in public transport terminals (IMPACT - Impact of Cultural aspects in the management of emergencies in public Transport), and crowd management at mass gathering events (LETSCROWD - Law Enforcement agencies human factor methods and Toolkit for the Security and protection of CROWDs in mass gatherings). Hermeneut shows that HF can deliver effective solutions to improve the security level of one organisation, by designing human contribution into the defence barriers. It is not enough to focus on hardware and software components. Organizations need to address HF aspects of cybersecurity by cultivating an informed and proactive workforce. Impact has analysed the role played by socio-cultural factors in the management of large groups of crowds in transport hubs i.e., airports, ports, underground and train stations, both in normal and emergency situations. Impact has applied a HF model to identify socio-cultural hazards that may affect crowd management in transport hubs and their potential consequences. The methodological approach provides a means for front-end operators to identify and discuss issues they encounter in their interactions with the public in transport hubs such as communication breakdowns with passengers due, for instance, to language barriers; misreporting of security threats; and uncooperative behaviour in case of emergencies. Let's Crowd aims to build an extension of the European security model especially thought for the protection of crowds during mass gatherings which builds upon the analysis of the human factors for designing security strategies and methodologies. HF methodologies will be used for developing supporting tools that will help security practitioners to prevent, anticipate and mitigate the criminal or terrorist attacks in mass gatherings.

Lynn Thiesmeyer (Keio University, Japan): ***Transboundary Community Security Issues in Southeast Asia: Monitoring Causes and Consequences.*** Within the research sites of Northern Myanmar, Laos, and Thailand, large rural populations seem left behind by the Sustainable Development Goals. Living along the borders, marginalized not only geographically but also in terms of the modern economy and social development, they are acutely, and not always positively, impacted by the advance of large-scale

development projects into their livelihood environments. Projects that convert large areas of land and water can bring about cumulative losses to the ecology and local livelihoods that are known as “slow-onset disasters.” These slower-evolving disasters, in turn, give rise to security threats, not only in terms of livelihoods but in terms of violent conflict as well. Such slower-onset security threats are reflected in low progress towards the SDGs, especially those of economic livelihood opportunities, health, and resilient, sustainable communities. They also contribute to, and worsen, rapid-onset disasters. In the example of the China – Myanmar border development project areas, long-term violent conflict results, due to increasing loss of resources. The specificity in geographic origin, and diversity in spread, of slow-onset disasters and security hazards make on-site, real-time field surveys imperative. In this situation our research relies increasingly on mobile technologies that can provide Small Data, with pinpoint spatial accuracy for peculiarities and minute changes in terrain along with pinpoint time data. Slow-onset disaster areas can, in this way, become accessible to quick and accurate prevention and response. Keywords: Southeast Asia, Transboundary, Rural, Low SDGs, Socio-ecological Systems

Dina Simunic (University of Zagreb, Croatia): ***Security Challenges of Applicable IoT Key Technologies in Health.*** The challenges in application of existing and future IoT key technologies are high, especially due to the fact that health is the most important category of human life. On one hand, IoT is already giving fantastic opportunities for following the personal health status, but on the other there is a significant risk related to possible stealing or misusing data or even misusing IoT network. Therefore, the paper discusses security and privacy of a recently developed system for IoT health, "Portable Medical Laboratory" (PmLAB), with Mobile Ad Hoc Networks as a self-configuring infrastructure for health data transmission. PmLAB is the IoT system operating with the server and data base, web application and mobile application. Data can be sent by wire or wirelessly, for example, by using Bluetooth Low Energy or WiFi modules. Medical doctor can reach the data base either via mobile or web app. Every patient has the corresponding identification number, which enables one-directional assignment. The patient can also use mobile application. In the paper, PmLAB system is initialized for every node to be considered untrustworthy. Behaviour of the nodes is being tracked, with the growing reputation. The nodes update continuously the other nodes' reputation. The overall reputation is stored in the central entity. The security has been checked for the part of the mobile application.

Ranjit Makkuni (Sacredworld Foundation, India): *The Betrayed IT Revolution* - *For those of us who have missed the IT revolution, consider yourselves lucky, we may not have missed a thing!* When the original vision of the Dynabook (later to become the laptop) was conceived by Alan Kay's team at Xerox PARC in the 1980s, computational tools were envisioned as a tool for creativity and leisure. Indeed the first slides of the Dynabook showed people freeing themselves from the shackles of their offices, lying in sprawling natural landscapes, pursuing their artistic creativity. Nearly 50 years later that vision has become a nightmare, with deep impacts on society: at levels of connection, health, psychological well-being, and deep questions to privacy and fundamental freedoms and 'Truth' loom and await answers. While in the past decade, social media addressed the human being re-'presented' as a collection of measurable and rapidly transportable artefacts (i.e., 'non material' computational files such as images, videos, text blurbs). But the idea of deep connection, palpable localized connection, in situ connection still haven't been addressed or have been ignored. Almost all of the world's civilizations have discovered or invented, after 1000s of years of 'traditional' social media innovation, the recognition of concepts such as site-based power places, sacred geography, and places of geomantic power, places of direct communion between Man and Natural forces. Many 1000s of years of observation, reflection and creativity, reflections of solar and lunar cycles, the motions of the planet earth around stars and its relative position with respect to planets, gave rise to a rich space and experience of rituals, fairs and festivals. The collective participation of physically present individuals in groups, large and small, situated in 'places' have never been addressed in modern media, except through the homogenized, limited formats of 'glass' computational screens. Indeed, social media forces people to disembody the world around themselves, become dislocated in order to access the benefits of access to large amounts of information. However, the benefits of Information access come at the risk of health and psychological issues. Indeed one could summarize the energy invested in virtual connection could be proportional to match the pain of societal alienation and ill health that result from people's primary communications with devices. Contentment and calm have been replaced by anxiety and constant displacement! With the rising power of evolving information technology, rapid changes that are taking place (with changes in 30 years being equivalent to changes in 300 years and more), smart cities exist with data-smart but emotionally un-smart, unhappy citizens. With rise of robotics and intelligent thinking machines, nations which have struggled with unemployment and poverty and who have just barely managed to remove poverty are suddenly confronted with the challenges of new unemployment resulting from

automation and confronted with new ways to reinvent themselves in an era of unpredictability and never ending change. These nations feel short-changed by the IT revolution because they have traded their ecological resources and traditional social capital in terms of harmonious communities and eco systems, in the promise of a 'smartness' revolution that has never delivered.

The question for us, as humanity, is to ask, when can we catch our breath and "just be?"

Add to this, governments in debt, honing the data powers of track individual's activities, widening tax nets by making banks into 'sensors and retinas', and the resulting invasion of privacy, the resulting questions of private property in the era of ubiquitous computing are open for reflection, discussion and new action. Fundamental questions on individual freedoms, that have been painstakingly achieved through spilling of blood and revolution seems to have gone in vain, especially considering that 'freedom' has been snatched away under the guise of surveillance. Amidst this new whirlwind of the IT revolution, new media, news, opinions presented on homogenized devices that 'occupy' peoples' eyes, hands, homes and offices, the minds of people can be easily manipulated. Not to mention the links between new media communication and the clutter of advertisements that occupy people's subconscious minds. Indeed we will need to rediscover Descartes' notion of "I [need to re-] think, [inorder to be who] I am". My paper asks the question, despite the positive advances of technology that have undoubtedly contributed to many dimensions in our lives, but, given the tremendous negative impact of people's health and well being, and rooted-ness, are we at a tipping point where we would need to rethink innovation afresh? Just as, in the past, across many cultures, people returning back into the solitude in the forests, connecting with local communities and sacred geography was an important ritual for renewal, can we, as an information society, re-learn perennial and fundamental values once again?

Quotes

- ALESSIA GOLFETTI (DeepBlue, Italy): *"When we work in complex systems we cannot deny the role of humans. Safe and secure performance should be cultivated at all levels. A shift from a technological centred perspective to a human centred approach is needed for looking at the entire ecosystem with people as part of that. As pointed out by the new strategic research agenda for the aviation domain, it is important to adopt a holistic approach where security is not only matter of technology, policy or procedures. It becomes effective only when it is able to ensure the human involvement*

throughout the overall lifecycle. Developing a culture of cyber awareness, organisations would be able to better handling cyber security threats."

- RANJIT MAKKUNI (Sacred World Foundation, India): "*With the rising power of evolving information technology, rapid changes that are taking place (with changes in 30 years being equivalent to changes in 300 years and more), smart cities exist with data-smart but emotionally un-smart, unhappy citizens.*"

More quotes from the workshop:

- LYNN THIESMEYER (Keio University, Japan): "*Mobile technologies work best when accompanied by mobile human capacities.*"
- NADIA SAAD NOORI (Teknova, Norway): "*Digitalization is receiving considerable attention for security, manufacturing and production with the aim of increasing effectiveness and boosting (European) industries and societal development (e.g. Industrie 4.0 in Germany; Brilliant Industry in Norway). Therefore, it is critical to develop the capacity in manpower and knowledge for enabling successful digital processes and services with pioneer capabilities in innovation.*"
- NADIA SAAD NOORI (Teknova, Norway): "*As the world is witnessing the Fourth Industrial Revolution , we at Teknova believe we a responsibility to bridging research with the technological trends. It is a strategic objective to bring leading edge ICT technologies and outstanding research ideas to industrial prototypes within the key markets of its partners and customers that are the energy, transport, and security sectors. As it is a core competence of Teknova to bring technologies like smart sensors, complex systems analysis, big data analytics, industrial mathematics for automation, digitalization and virtualization of processes to many; we also make sure that our solutions address the needs of promoting a culture of responsible integration of technology towards safer working and living environments. "*
- SARAH JANE FOX (Middlesex University, United Kingdom): "*The central public service in a modem state remains the police. Advancing technology and the digital infrastructure are essential components for keeping citizens safe and secure. The use of such technology has become essential, and yet, there is an expectation that the service will also 'police' much of the technology going forward – such as artificial intelligence, autonomous vehicles and drones – without suitable (and consistent) framework and approaches being established. There must be clear guidance, legislative controls and supporting infrastructure put in place for advancing technology - its use, and for any offences and breaches that may subsequently occur." - "The positive use of technology must be promoted; when used by the police,*

technology, such as drones – can save lives and enhance security. This requires constructive communications (including through social media) to ensure that this is emphasized to the public and misconception and inaccuracies do not undermine the use and advantages of such."

- PAVAN DUGGAL (Pavan Duggal Associates, India) : "*Cybersecurity is a paramount factor for all stakeholders today. However regulations on cybersecurity starts bringing forward large number of legal, policy and regulatory challenges which need to be adequately addressed both at international and national levels*"
- RANJIT MAKKUNI (Sacred World Foundation, India): "*But, ideas of deep connection, palpable localized connection, in situ connection still have not been addressed or have been ignored by the Web*".
- RANJIT MAKKUNI (Sacred World Foundation, India): "*The benefits of Information access come at the risk of health and psychological issues. Indeed, one could summarize the energy invested in virtual connection could be proportional to match the pain of societal alienation and ill health that result from people's primary communications with devices*".
- RANJIT MAKKUNI (Sacred World Foundation, India): "*The body has been dematerialised andctively disembodied! Contentment and calm have been replaced by anxiety and constant displacement!*"
- RANJIT MAKKUNI (Sacred World Foundation, India): "*Just as, in the past, across many cultures, people returning back into the solitude of the forests, connecting with local communities and sacred geography was an important ritual for renewal, can we, as an information society, re-learn perennial and fundamental values once again?*"

II. Overall outcomes of the session highlighting

There is a need to identify a reference point for researchers, companies and involved stakeholders in the field of ICTs for safety, security and disaster recovery/management. The role of reference point can be perfectly carried out under the umbrella of the WSIS.

There is as well a need to promote an interdisciplinary debate on the implementation of the information society in the light of a social, ethic, economic, healthy long term perspective.

The implementation of the WSIS action lines beyond 2015 must adequately take into account the dynamic evolution and reshaping of technologies posing new problems and

sometimes concerns at an increasing pace. If universal goals, representing universal general values, may be valid for a long period of time, action lines use to refer to specific fields and strategies and, as a consequence, must adapt time to time to the evolving scenario.

III. Main linkages with the Sustainable Development Goals

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

Goal 2: End hunger, achieve food security and improved nutrition and promote sustainable agriculture
Goal 3: Ensure healthy lives and promote well-being for all
Goal 6: Ensure access to water and sanitation for all
Goal 7: Ensure access to affordable, reliable, sustainable and modern energy for all
Goal 8: Promote inclusive and sustainable economic growth, employment and decent work for all
Goal 9: Build resilient infrastructure, promote sustainable industrialization and foster innovation
Goal 11: Make cities inclusive, safe, resilient and sustainable
Goal 16: Promote just, peaceful and inclusive societies
Goal 17: Revitalize the global partnership for sustainable development

More in detail:
SDG 2 END HUNGER, ACHIEVE FOOD SECURITY AND IMPROVED NUTRITION AND PROMOTE SUSTAINABLE AGRICULTURE - > food & water security

SGD 3 ENSURE HEALTHY LIVES AND PROMOTE WELL-BEING FOR ALL AT ALL AGES
3.d Strengthen the capacity of all countries, in particular developing countries, for early warning, risk reduction and management of national and global health risks -> Safety & Security

SDG 5 ACHIEVE GENDER EQUALITY AND EMPOWER ALL WOMEN AND GIRLS
5.b Enhance the use of enabling technology, in particular information and communications technology, to promote the empowerment of women -> human security, safety

SDG 6 ENSURE AVAILABILITY AND SUSTAINABLE MANAGEMENT OF WATER AND SANITATION FOR ALL

6.a By 2030, expand international cooperation and capacity-building support to developing countries in water- and sanitation-related activities and programmes, including water harvesting, desalination, water efficiency, wastewater treatment, recycling and reuse technologies -> Water Security, critical infrastructure resilience, etc

SDG 7 ENSURE ACCESS TO AFFORDABLE, RELIABLE, SUSTAINABLE AND MODERN ENERGY FOR ALL

7.b By 2030, expand infrastructure and upgrade technology for supplying modern and sustainable energy services for all in developing countries, in particular least developed countries, small island developing States, and land-locked developing countries, in accordance with their respective programmes of support -> C5, critical infrastructure resilience, etc.

SDG 8 PROMOTE SUSTAINED, INCLUSIVE AND SUSTAINABLE ECONOMIC GROWTH, FULL AND PRODUCTIVE EMPLOYMENT AND DECENT WORK FOR ALL

8.3 Promote development-oriented policies that support productive activities, decent job creation, entrepreneurship, creativity and innovation, and encourage the formalization and growth of micro-, small- and medium-sized enterprises, including through access to financial services -> C5 safety & security

SDG 9 BUILD RESILIENT INFRASTRUCTURE, PROMOTE INCLUSIVE AND SUSTAINABLE INDUSTRIALIZATION AND FOSTER INNOVATION

9.1 Develop quality, reliable, sustainable and resilient infrastructure, including regional and transborder infrastructure, to support economic development and human well-being, with a focus on affordable and equitable access for all

9.a Facilitate sustainable and resilient infrastructure development in developing countries through enhanced financial, technological and technical support to African countries, least developed countries, landlocked developing countries and small island developing States

9.c Significantly increase access to information and communications technology and strive to provide universal and affordable access to the Internet in least developed countries by 2020 -> C5, critical infrastructure resilience, etc etc

SDG 11 MAKE CITIES AND HUMAN SETTLEMENTS INCLUSIVE, SAFE, RESILIENT AND SUSTAINABLE

11.4 Strengthen efforts to protect and safeguard the world's cultural and natural heritage -> extended cooperation with UNESCO

11.5 By 2030, significantly reduce the number of deaths and the number of people affected and decrease by [x] per cent the economic losses relative to gross domestic product caused by disasters, including water-related disasters, with a focus on protecting the poor and people in vulnerable situations -> C5 Safety and Security

11.b By 2020, substantially increase the number of cities and human settlements adopting and implementing integrated policies and plans towards inclusion, resource efficiency, mitigation and adaptation to climate change, resilience to disasters, and develop and implement, in line with the Sendai Framework for Disaster Risk Reduction 2015-2030, holistic disaster risk management at all levels -> C5 Safety and Security

SDG 16 PROMOTE PEACEFUL AND INCLUSIVE SOCIETIES FOR SUSTAINABLE DEVELOPMENT, PROVIDE ACCESS TO JUSTICE FOR ALL AND BUILD EFFECTIVE, ACCOUNTABLE AND INCLUSIVE INSTITUTIONS AT ALL LEVELS

16.2 End abuse, exploitation, trafficking and all forms of violence against and torture of children -> C5 safety & security

16.5 Substantially reduce corruption and bribery in all their forms -> C5 safety & security

16.10 Ensure public access to information and protect fundamental freedoms, in accordance with national legislation and international agreements -> C5 safety & security

16.a Strengthen relevant national institutions, including through international cooperation, for building capacity at all levels, in particular in developing countries, to prevent violence and combat terrorism and crime -> C5 safety & security

SDG 17 STRENGTHEN THE MEANS OF IMPLEMENTATION AND REVITALIZE THE GLOBAL PARTNERSHIP FOR SUSTAINABLE DEVELOPMENT

17.8 Fully operationalize the technology bank and science, technology and innovation capacity-building mechanism for least developed countries by 2017 and enhance the use of enabling technology, in particular information and communications technology -> C5 safety & security

17.16 Enhance the global partnership for sustainable development, complemented by multi-stakeholder partnerships that mobilize and share knowledge, expertise,

technology and financial resources, to support the achievement of the sustainable development goals in all countries, in particular developing countries -> C5 safety & security

17.17 Encourage and promote a active public, public-private and civil society partnerships, building on the experience and resourcing strategies of partnerships. -> C5 safety & security

IV. Emerging Trends related to WSIS Action Lines identified during the meeting

C5, C7

DINA SIMUNIC : The overview and offered solutions related to security challenges of applicable IoT key technologies in the health sector shows that there is a lot of concern, but at the same time also care for the citizens' privacy and security. This is especially the case now in EU, due to the close date of GDPR enforcement, with its data subject rights, especially in the application of privacy by design in coming future communications systems.

C5,C7

HAYLEY WATSON: ICT's are almost certainly a powerful tool in building citizens resilience to crises, and have certainly contributed to societal changes with regard to their uptake and impact, as the world of crisis informatics has shown. Yet, it is important to go beyond a technological determinist view of ICTs in this realm, to a wider consideration of the organisations, economic and social considerations that impact uptake and therefore their usefulness.

C6,C7,C8,C10

LYNN THIESMEYER: Change, motion, and dynamism in environments, populations, and events can be digitally captured in short time "frames." How can we capture the longer-term changes, movements and events that are part of slow-onset disasters and their security threats?

C5, C7

NADIA SAAD NOORI: We are witnessing a multifaceted digital revolution with high-performance computing, broadband communication, sensing and artificial intelligence integrated in our daily human life. As the lines of separation between the physical and digital worlds are blurring, societies in the digital age became more complex and a host of new vulnerabilities emerged with this borderless digital medium. Freedom and

connectivity was the bright side of a digital age connecting cyber and physical worlds (e.g. IoT, UAV). Unfortunately, a dark side is hidden away in the corners of the dark web where criminals and terrorist organization exploited such tools for malicious purposes. Therefore, we are have a responsibility to invest in the developing the tools and means to tackle the vulnerabilities brought by the digital revolution and address their impact on the physical world and the human life.

C3,C4,C5,C6,C8,C10

RANJIT MAKKUNI: The betrayed revolution - My thoughts for some time have circled around how the speed of the new information revolution renders us less capable of critical thought, due to all the constraints placed upon us with new technologies. For instance, as liberating as they are - by providing flexibility and instant connectivity - we have become enslaved to our devices, fearful of losing out information and access in an increasingly competitive and fast-paced world. Consequently, our bodies have suffered, as have our minds (due to information overload), what of our work-life balance -- and this is just to begin with!

What if we can connect with like-minded colleagues all over the world to discuss how we may begin to shift this paradigm, and how technologies can be a central aspect of our lives without owning us. As you discussed, there are several initiatives in various parts of the world (your session at WSIS included) that are doing this in their own way. Can these initiatives be connected or brought together to make this a stronger voice, stronger demand? Can we start the process at WSIS 2018 and build the momentum for next year? Civil society and citizens' voices are increasingly being compromised in many ways and at many fora. Can we use this opportunity to our advantage and begin to think of changing the tide?

V. Suggestions for Thematic Aspects that might be included in the WSIS Forum 2019

ALFREDO M RONCHI: To include and promote a wider range of “security” topics under the WSIS umbrella endorsing a holistic approach to the “Safety, Security, Disaster Recovery and Management” sector.

ALFREDO M RONCHI: Ethic and Juridical aspects concerning the extended use of artificial intelligence (e.g. e-Transportation, e-Health, e-Government …).

NADIA SAAD NOORI: The artificial intelligence and the perils of mathematical equations biases. How can we ensure AI algorithms and training datasets will not produce decision based on race or stereotyping? Humans in the physical world have been fighting for decades such biases, so how can we import these principles to the digital world to teach the AI algorithms? For the sake of safer, secure and balanced societies! ”

PAVAN DUGGAL: Protection and preservation of cybersecurity.

RANJIT MAKKUNI: Rethinking the role of digital technologies for a human centred society.

Please complete this document and send to Matthew L. Greenspan, Matthew.Greenspan@itu.int AND Gitanjali Sah, Gitanjali.Sah@itu.int