Position Paper 'Security & Safety'

An Introduction to Security & Safety

Balance between opportunity and threat

Historically, all human progress has created both opportunities and threats. New tools, products, technology and even non-physical developments like ideas, organizational structures and methods are initially developed to help the world take a step forward. But unfortunately, every new development also brings new threats: threats because of failure of a system or because of its use by the wrong people. Aircraft, trains and cars are involved in accidents. Tools become weapons.

In the past decade, change has speeded up dramatically. Information and Communication Technology (ICT) has been the engine behind immense developments, not only technical but also organizational. Globalization not only brings progress and opportunities, but also scales up the threats.

In the right hands, IT can be a powerful tool to prevent danger and to fight threats of all kinds. On the other hand we need to be aware that IT itself, like any other development, introduces new threats, since it can fail or be used by the wrong people.

In the Security & Safety track, we will address situations where IT is used as a powerful instrument helping authorities in their fight against threats. At the same time we will not ignore the dangers that are introduced by the use of IT itself.

Why is this domain important and why is there a separate track for it at the WCIT2010? The reason is both simple and urgent: the dependence of the world on IT for better safety has become 'mission critical' in all areas of society. We simply cannot afford to sit back and wait.

The WCIT2010 theme 'Challenge for Change' means we all have to work together to make sure that the balance between opportunities and threats is moving in the right direction.

Inspiration

The challenges in security & safety

In tomorrow's world, safety standards will demand that we ensure the best possible protection, while allowing maximum personal freedom in private and public buildings, shopping areas, public transportation, and that we secure a sound infrastructure. Safety solutions should enable an efficient, secure flow of people, goods, vehicles, capital and information offer the most attractive options for private investors, international and regional organizations, residents, tourists and more.

The drivers are megatrends such as urbanization, demographic change, ecological change and globalisation.

Today, around 300 million people live in megacities (> 10 million). For the first time in human history, more people live in cities than in rural areas. The numbers are growing: In 2015, more than 350 million people are expected to be living in megacities. Safety and security come second only to transportation infrastructure as factors contributing to the competitiveness of a city (city rankings). Major terrorist attacks like 9/11 and the London Metro bombings are in everybody's mind.

The world's population continues to grow rapidly and to age. By 2025, the world's population is expected to reach around eight billion. Low birth rates, combined with longer life expectancy worldwide lead to ageing societies – the world's fastest-growing population segment is the over-60 age group. Against this background, one of our greatest challenges is to create a safe and viable infrastructure (energy, water, industry, transport, capital) for billions of people.

The amount and impact of natural disasters and hazards is increasing. The tsunami of 2004 and hurricanes like Katarina caused many casualties and disrupted total infrastructures. The consequences still are influencing daily life in those places. This leads to an increasing need for predictive technologies, widespread warning systems and integrated and scalable command, control and communication infrastructures.

The world is becoming more interconnected – not only through new technologies, but also in economic and logistical terms. The volume of goods traded in 2004 was nearly triple that of 1950. Globalization is a process that is politically and economically desirable and technology-driven. It promotes fair competition, open markets and cooperation among all nations and cultures. It tends to be most perceptible and observable in almost every facet of life, mainly due to the emergence of internet technology. Today, we are surrounded by a multi-level convergent media world where all modes of communication and information are continually reforming to adapt to the enduring demands of technologies, changing the way we create, consume, learn and interact with each other.This cyberspace creates

multiple virtual identities which represent real people. As in real life, there is a need for safety in cyberspace. Secure communities are needed, based on solid connections between the real and virtual world. People must be able to trust processes and solutions in place at financial institutions (compliance), in government (electronic ID's), and at public digital locations like Facebook, Hyves, etc.

Day 1

Presentations on day 1 will focus on challenges in IT safety and security based on three levels of concern: 1. Society: How does it affect cities, citizens and commercial enterprises? 2. The single business level: What is the impact on operations (financial institutions, transport & industry) and fraud (cyber security) 3. The individual level: How to protect identity and privacy.

Innovation

SOLUTIONS, NOW AND IN THE FUTURE

Innovation within public safety is the domain of hundreds of technologies: voice, data and video communications, physical, network and biological sensors, geospatial intelligence and analytical models, incident command and operations, center management and biometric access control, not to mention hazard forecasting and vulnerability analysis, handheld wireless data sharing, visualization and situational awareness, computer-aided dispatch, collaboration and planning, surveillance and smart video analytics ("fingerprinting").

Basically all activities to build safe communities fit into the following cycle:

The goal of activities in **PREPARE** is to **prevent** threats from materialising and to **prepare** people and organizations for events.

Collecting, sharing and analyzing information are powerful tools in this phase. Exercises and training in accordance with pre-defined scenarios not only help people to get ready for action, but also reveal the weak spots in the (cooperative) plans. Sensor technology is used to collect information where human observation is impossible or inadequate. Early warning and alerting systems help both organizations and individuals to prepare for situations that are (or might be) dangerous.

Physical, technical and organizational measures to protect vital infrastructure (e.g. in the energy, water, chemical, industry, food, transport, financial and communications sectors) and information need constant attention, since our dependence on these is obvious, while people and organizations with malicious intents are becoming more and more creative, even innovative, in breaking down this protection. In this area, ID-control, authentication and authorization all use innovative solutions, such as biometrics. Fighting cybercrime is part of this activity.

ACT is about command and control in dangerous situations, whether these are unforeseen, foreseen or maybe even planned.

During ACT, making the right decisions is vital. The (semi-)static information collected during PREPARE is supplemented with up-to-date, operational, information. Geospatial presentation helps people quickly understand a common operational picture. Emergency response, intelligence-led policing, evacuation and guiding people at mass events like the Olympics all depend on accurate, up-to-date information, shared over trusted and solid communication networks, to make sure that well-prepared and trained people can take the right action.

During ACT, collection of information continues, not only to control the situation, but also as a link to the next phase, EVALUTE.

EVALUATE starts with building the best possible view of what happened during ACT. This often calls for combining information in new ways.
The main purpose is evident: to use the lessons learned in order to prepare more effectively for similar future events. Often, another objective is to be able to effectively prosecute those responsible for the event. Collecting and interpreting evidence also involves investigating the IT and communication tools of the 'enemy'.
Assuring a solid 'chain of custody' is becoming more important, since criminal and terrorist organizations are creative in using the gaps in the law, especially when more than one country is involved.

Day 2:
Presentations on Day 2 will typically be about solutions that support at least one of the stages in the above schedule. We also aim to obtain examples spread over the 3 levels of communities (global/national, regional/cities/enterprises and individuals) mentioned in **Inspiration.** Ideally, the presentations will be by representatives of organizations that 'own' the issues, combined with the provider of the solution.

Transformation

MAKING IT WORK TOGETHER

What is Transformation? Transformation is the process of making innovative solutions work to beat the challenges.

Public Private Partnership, Braking the walls
The most typical aspect of threats is the fact that they are not confined by physical or organizational boundaries. The only way to fight them effectively is by working together.
Since the world increasingly depends on complex structures, improving safety and security calls for more cooperation. This often involves cooperation between organizations that never expected to work together. Dedicated safety-related organizations work together with organizations that have their core business in the other tracks of WCIT2010. The urgent need for public and private organizations (including scientific institutes and NGO's) to operate together is becoming increasingly clear. This often means that organizations and people have to give up long held privileges.
A clear example of this can be found in the area of cyber forensics. The increasing complexity and miniaturization of microchips and the complexity of the various communication protocols used on the internet drive forensic investigators all over the world to cooperate with soft- and hardware vendors in order to guarantee safety and security to the citizens of our society.

Public Private Partnership, Funding projects
The speed of technology replacement cycles means that it is increasingly less economical to buy technology outright, and the trend toward some form of payment-for-use is increasing, often backed by some kind of asset finance.
There is also a fundamental and growing need for the public services to involve private finance in order to afford critical investments. The public-private partnerships through which such financing is being structured are traditionally thought of as equity participation in major projects. However, this definition is now being widened to include any partnership where the private sector takes on an element of the risk associated with a project, large or small.
Involving private finance is not simply a strategy to secure funds, but is also a matter of introducing commercial efficiency, process discipline, technological knowledge and more effective, transparent decision making.

Privacy Protection
In the transformation process, the balance between interests of the society and of the individual is often at stake. The need for information in order to be able to prevent incidents often affects privacy. A constant discussion has to keep us all alert to make sure that we all have a common understanding of what is allowed and what is not. In order to implement the solutions, this common understanding has to be translated into clear and broadly supported rules and legislation.

Program management (Business as usual)

IT Transformation is about comprehensive design, planning and implementation of individual transformation measures, as well as the overall control and management of organisational change. In the security and safety business, IT is increasingly becoming a driver of organizational and process change. Conversely, adapting systems and workflows, as well as organizational structures and the way in which people work, are critical to success. In many cases, a simultaneously initiated cultural change is the key to sustainable business improvements.
One of the critical success factors for IT Transformation is professional program management. Transformation should be managed as a program, with each core process, its related applications, and the overall infrastructural integration run as separate projects. Generally, IT Program Management covers the following activities: program set-up, program execution, program support processes and program closure.

Day 3:
Presentations on Day 3 will typically be about implementing the solutions raised in **Innovation**. The focus is on 'how to make it happen'. Ideally, the presentations will be by representatives of organizations that 'own' the solutions, combined with the provider of the solution.