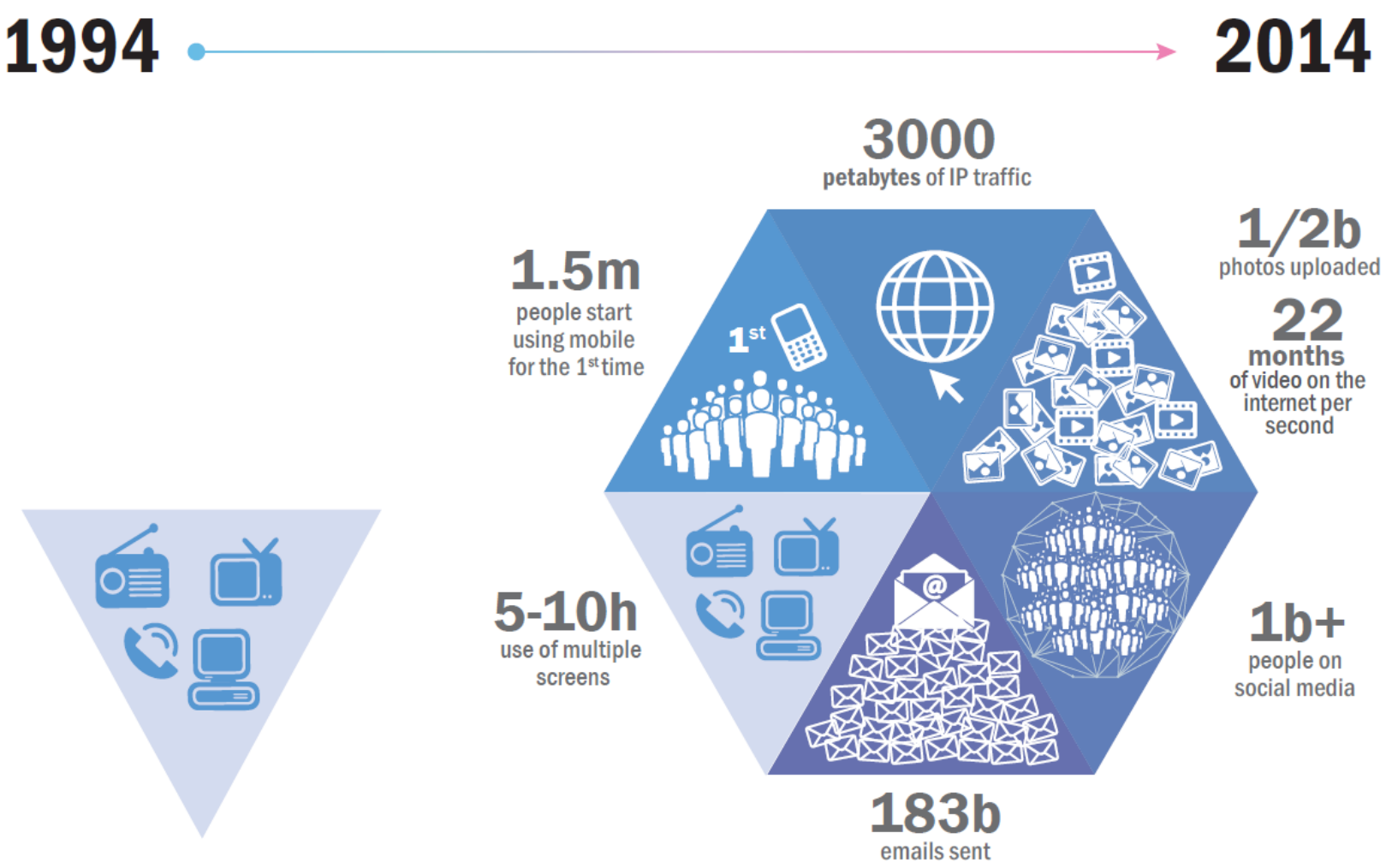
# Smart Sustainable Cities

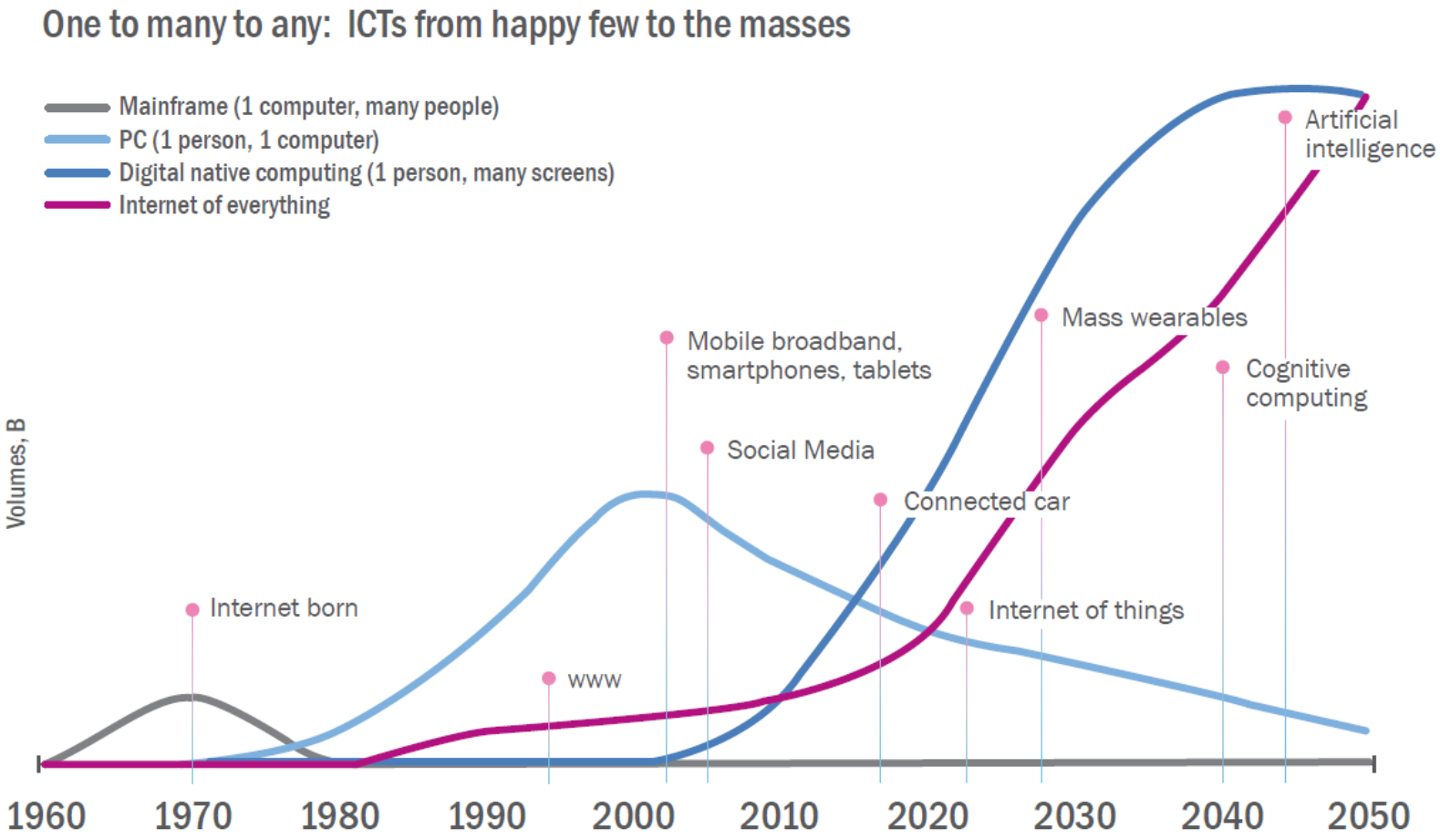
## The ICT Policy & Regulatory Context

# A day in the [digital] world



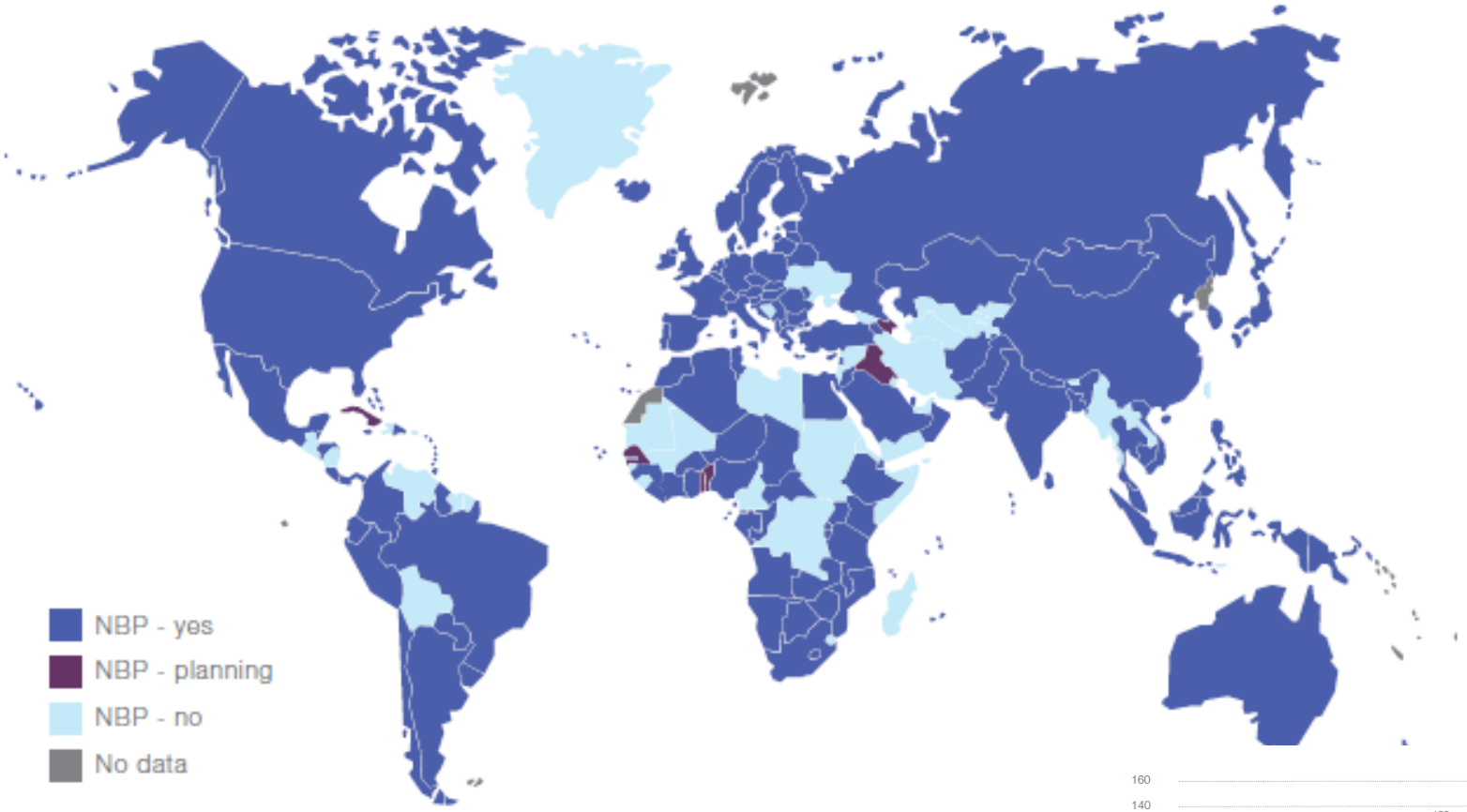

Source: ITU

# History of the future




Source: ITU

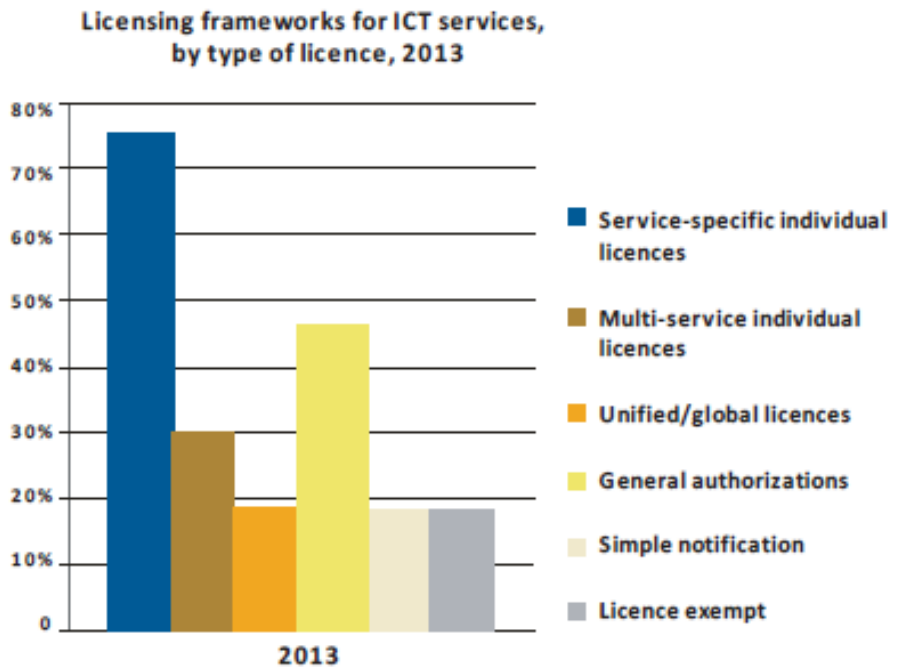
# National Broadband Plans and Policies……

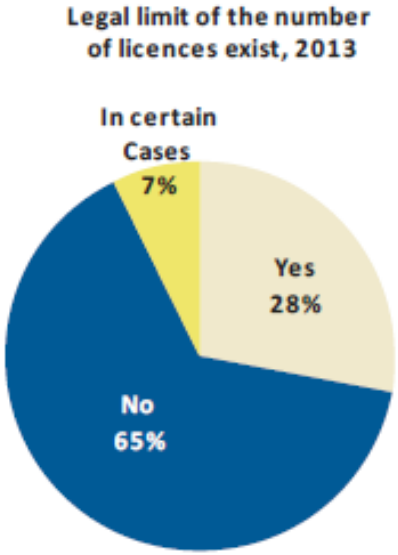



Source: ITU World Telecommunication/ICT Regulatory Database; The State of Broadband 2013 (forthcoming). Co
Include Azerbaijan, Benin, Cape Verde, Comoros, Cuba, Iraq, Marshall Islands, Micronesia, Senegal, Solomon Isl

# Licensing framework

**Figure 1.8: Licensing frameworks for ICT services, 2013**

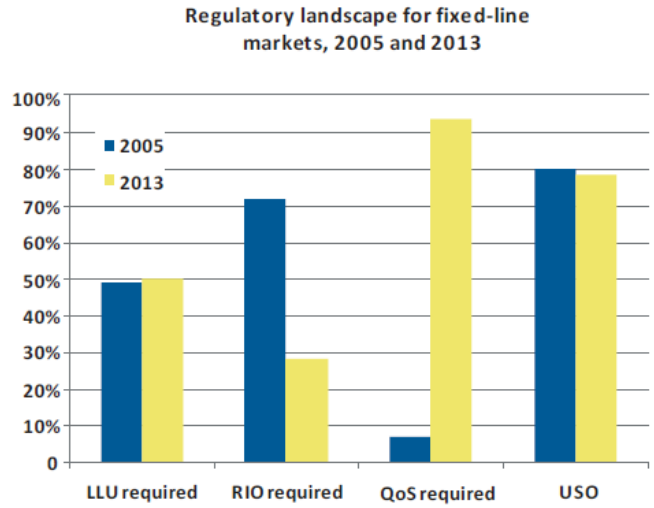


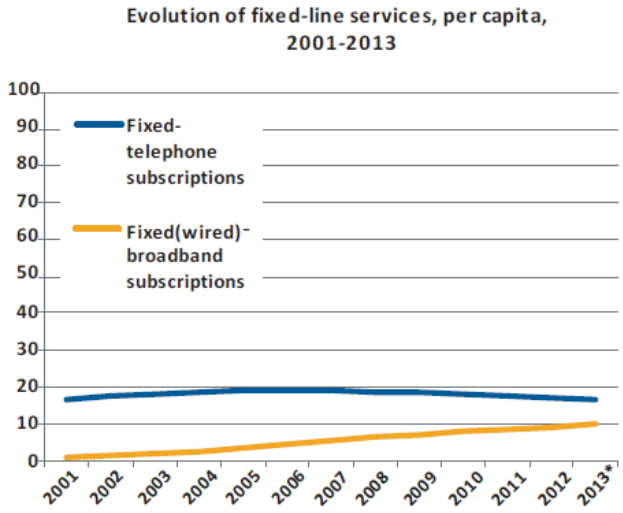




*Source: ITU, www.itu.int/icteye.*

# Regulating fixed line services

**Figure 1.6: Regulating fixed lines**



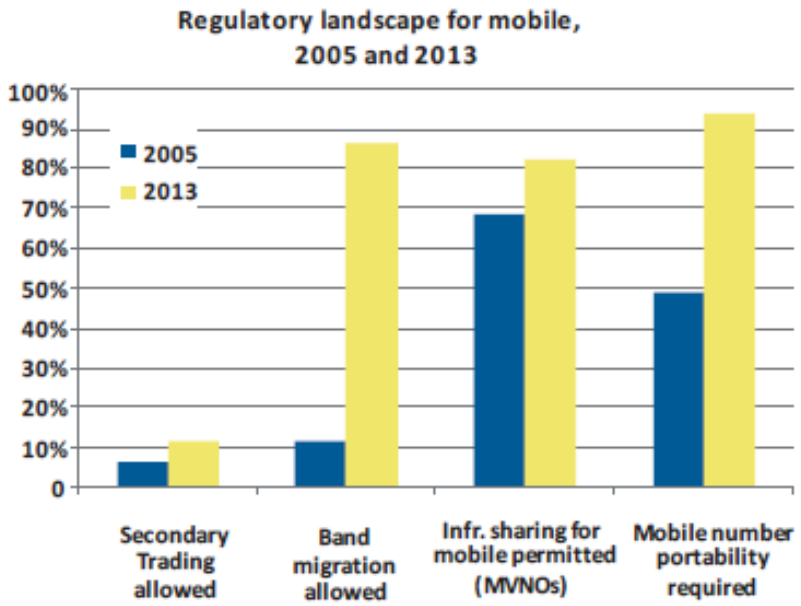

*Legend:* *LLU = Local Loop Unbundling*
*RIO = Reference Interconnection Offer*
*QoS = Quality of Service*
*USO = Universal Service Obligations*

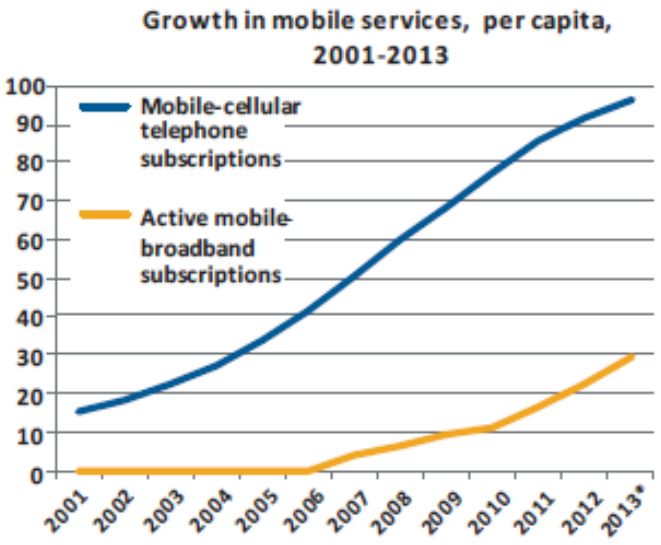
*Note: * estimates.*

*Source: ITU, www.itu.int/icteye.*

# Regulating Mobile Services

**Figure 1.7: Incentive regulation and growth in mobile services**




*Note: * estimates.*

*Source: ITU, www.itu.int/icteye.*

# Definition of SSC

"A smart sustainable city is an innovative city that uses information and communication technologies (ICTs) and other means to improve quality of life, efficiency of urban operation and services, and competitiveness, while ensuring that it meets the needs of present and future generations with respect to economic, social and environmental aspects".

- ITU-T Focus Group on Smart Sustainable Cities (FG-SSC)



FINANCIAL TIMES

March 11, 2015 12:01 am

# Iniesta teams up with Telefónica to back wearable tech start-up

Daniel Thomas, Telecoms Correspondent Author alerts

Barcelona football player Andrés Iniesta and NBA basketball player Serge Ibaka are teaming up with telecoms group Telefónica to back a Spanish wearable technology company whose device gives sports fans the player's point of view.

FirstV1sion has created a T-shirt with a camera embedded at chest level to provide broadcast-standard video, as well as feedback on the player for the team to monitor.

Wearable sports technology is a part of the wider "internet of things" market, which is attracting increasing levels of investor interest. California smartwatch maker Pebble set a record on Kickstarter, the crowdfunding platform, raising more than $17m in less than a month.

While most major technology groups are focusing on health-monitoring wristbands and watches, others are developing jewellery, glasses, shoes and clothes that can provide feedback on movement as well as communication methods.

Telefónica has invested €60,000 for a 7 per cent stake in FirstV1sion and supported it through Wayra, its start-up accelerator.

The start-up now hopes to raise up to €5m on BankToTheFuture, a peer-to-peer crowdfunding platform, to fund its next stage of growth.

The device has been tested by players in Barcelona training sessions as well as by referees in a match between Real Madrid and Barcelona. The content was distributed by 150 broadcasters worldwide.

Telefónica owns MovistarTV and has a stake in Canal+, two of Spain's main sports broadcasting companies, and has bought the media rights for Barcelona next year.

FINANCIAL TIMES

Home World Companies Markets Global Economy Lex Comment Management Life & Arts

Africa | Asia-Pacific | Europe | Latin America & Caribbean | Middle East & North Africa | UK | US & Canada | The World Blog | Tools

Last updated: October 30, 2014 5:17 pm

# Bristol to become smart city laboratory

John Murray Brown

The underground ducts that brought cable television to Bristol in the 1970s are being upgraded as part of an ambitious project to create a living laboratory for research into the future of cities.

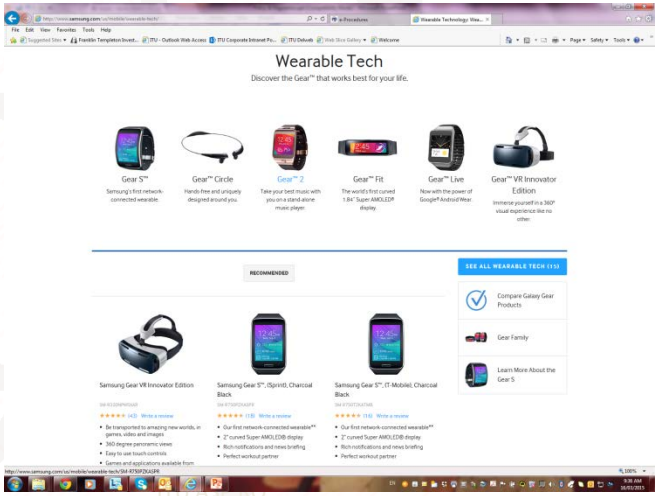
As part of a £75m joint experiment carried out by the city council and the University of Bristol, the old Rediffusion infrastructure, which runs for 100 miles under the streets, is being fitted out with superfast, high-capacity fibre funded under the government's superconnected cities programme.

For a fee, telecommunications equipment companies and mobile app start-ups will be able test new products and services on the network on a city-scale under live conditions. Areas that could be researched include future mobile phone networks, new apps, traffic flow – and thus pollution control and the potential for driverless cars – smart power grids and metering, and remote healthcare.

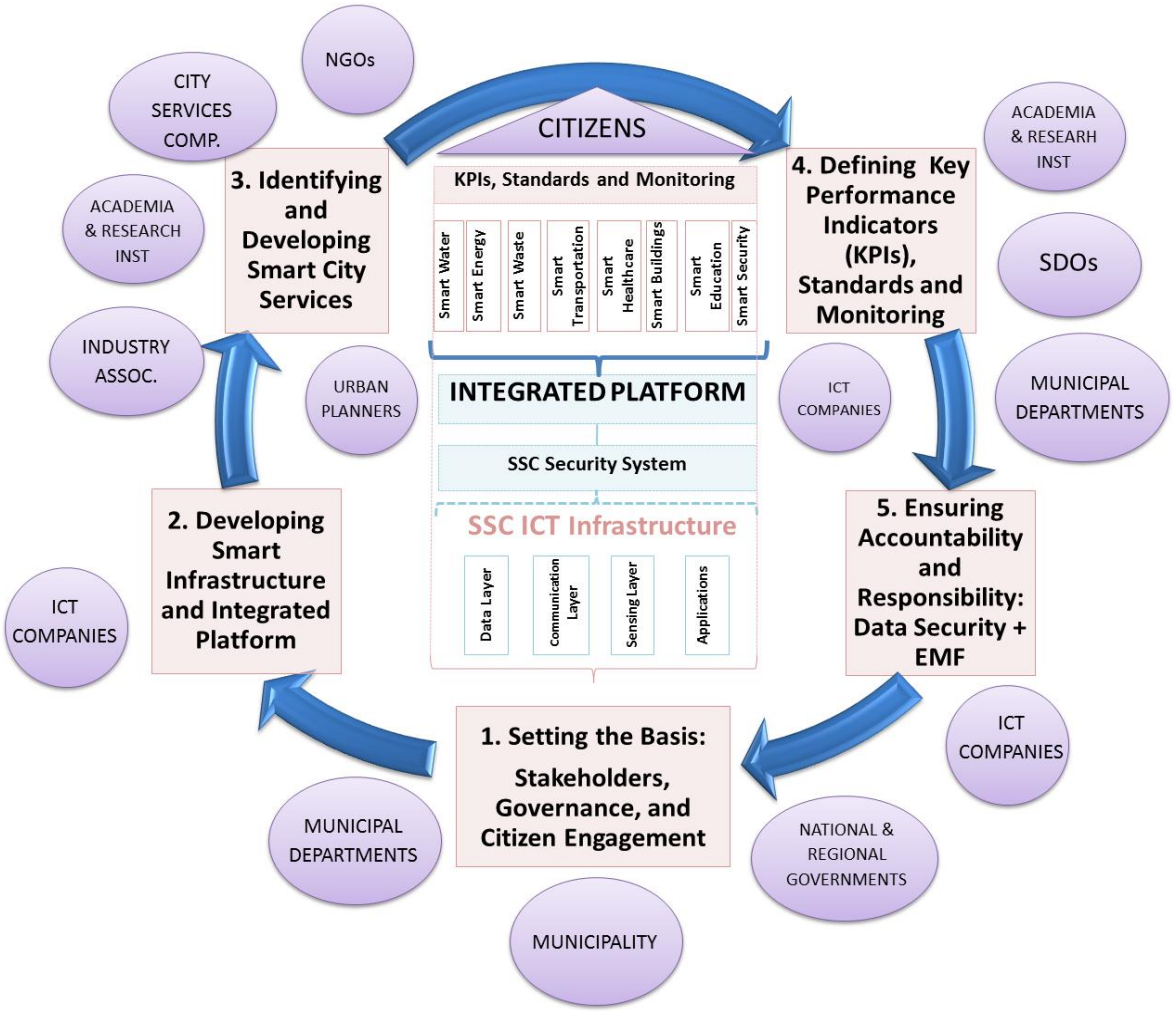
The initiative is being promoted by George Ferguson, who when elected Bristol mayor as an independent in 2012, vowed to make the city a "laboratory for change". It puts Bristol at the forefront of the so-called smart city debate, which is driven by the global trend towards urbanisation, the growth of mobile communications and the prevalence of devices such as sensors to create new sources of data – sometimes called the internet of things.

"Managing the internet of things requires different forms of networking," says Paul Wilson, the council official in charge.

Professor Dimitra Simeonidou, the project's chief technical officer, who heads Bristol university's high-performance networks research


# Smart Sustainable Cities: Stakeholder Map



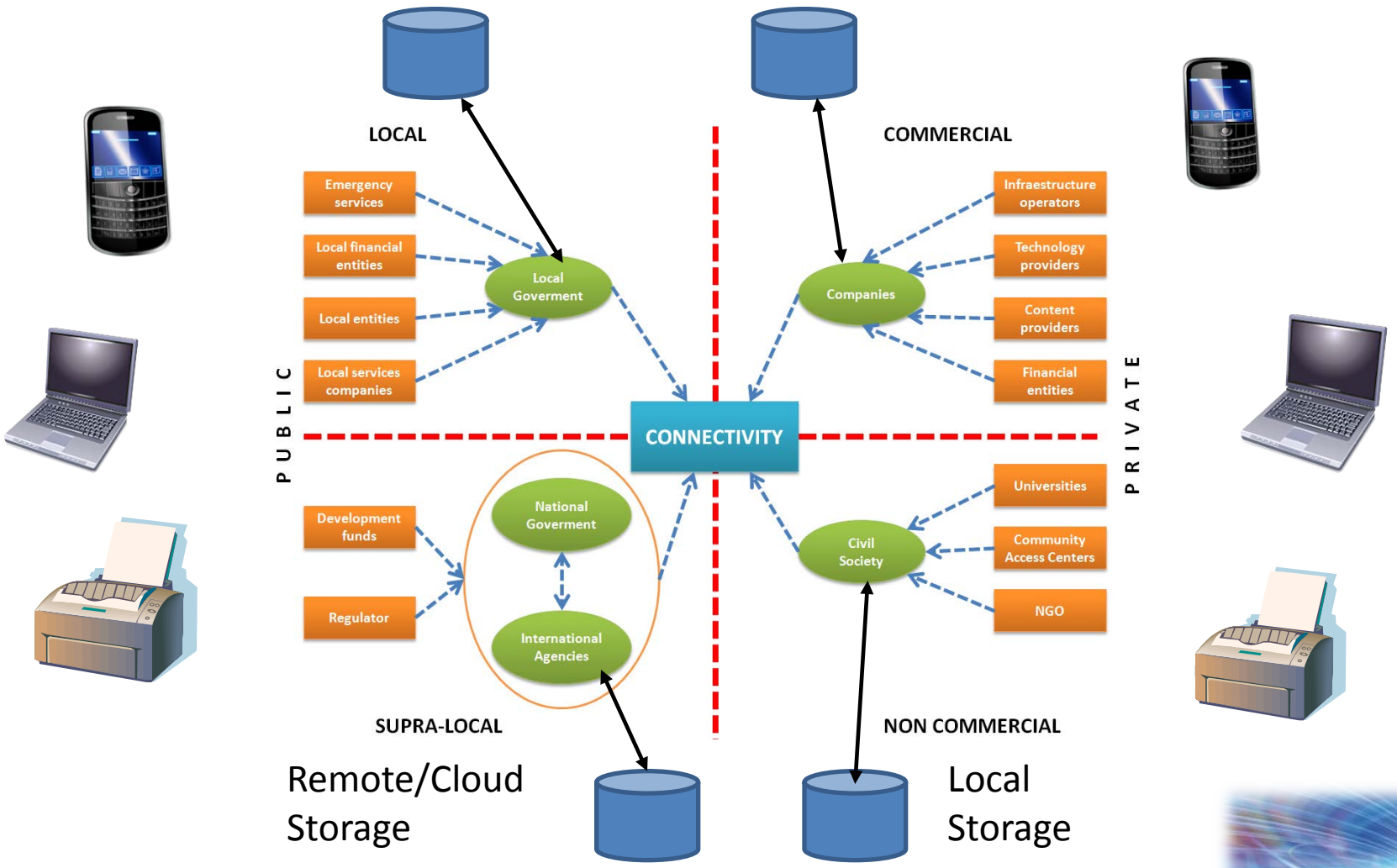

The citizens are the top, as the users of the cities the ultimate purpose of SSC

ICT companies can be seen as the glue that, with the ICT infrastructure and the city platform, ties together the system

NGOs, urban planners, in constant contact with the citizens act as an input into the development of SSC initiatives

Source: FG-SSC "Technical Report on Stakeholders for Smart Sustainable Cities", page 22

# ICT Infrastructure Landscape for SSCs




Sources: Adapted from FG-SSC "Technical Report on Smart Sustainable Cities Infrastructure" Page 11 and Ministry of Transportation and Communications of Peru

# IMPROVING QUALITY OF LIFE..


Emergency


Education


Health


Agriculture

Governance


Investment


Applications


Policy & Regulation


Capacity Building


Transport


Sensor Networks


Universal Broadband


Green ICT & E-Waste


Measurements


Electricity


Infrastructure Security


Privacy & Security


Water



Digital Inclusion

## SMART SUSTAINABLE CITIES


Spectrum Management


Standards, Conformity & Interoperability


Teleworking

# Different Services, Different Requirements - Examples

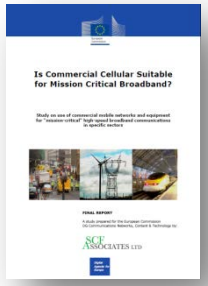
## PPDR services

- **Constant availability** –
- **Ubiquitous coverage** – not just outdoors, but inside buildings (including large ferroconcrete structures such as shopping malls) and in tunnels (including subways).
- **Regionally harmonised spectrum** –
- **Differentiated priority classes** .
- **Support for dynamic talkgroups,**
- **Automatic identification with authentication.**
- **Automatic location discovery and tracking**
- **The ability to maintain connectivity**
- **Fast call setup** (<200ms) and immediate access on demand: the **Push-to-talk** (PTT)function and **all-calls** (internal broadcasts).
- **Relay capabilities**
- **Support for Air-Ground-Air (AGA) communication** when and where needed.
- **Adequate quality of service**
- **The ability to roam onto commercial networks**
- **Interworking between various PPDR services,** and increasingly, across borders.

## Utility industry :

- **Teleprotection** – safeguarding infrastructure and isolating sections of the network during fault conditions whilst maintaining service in unaffected parts of the network.
- **Data monitoring** via SCADA (Supervisory, Control And Data Acquisition) systems.
- **Automation** – systems to autonomously restore service after an interruption or an unplanned situation.
- **Security** – systems to ensure the safety and security of plant.
- **Voice services** –.
- **Metering** – collecting data from smart meters and communicating with them for various reasons, such as demand management and to implement tariff changes.
- **Connectivity** – telecommunication networks to interconnect the above services in a reliable and resilient manner under all conditions.
- Other operational requirements include:
- **Coverage of all populated areas with points of presence throughout the service territory**
- **Costs must be low**
- **Continuity of service is vital,** and price stability
- **Utilities want network separation,**

## Intelligent Transport Services… *and more*



**What type of network is required to deliver these services?**

- Private networks
- Public networks

**What preparations are required to make best use of commercial networks to deliver smart services (some of them such as Emergency Telecommunication, Utilities, Transportation critical in character)?**

- Technical (e.g. coverage, resilience, quality, spectrum, interoperability)
- Commercial (e.g. availability, long term pricing, SLAs
- Policy & Regulatory (e.g. critical services as priority, quality of service, long term tariffs, security, privacy, USO, infrastructure sharing, licensing)

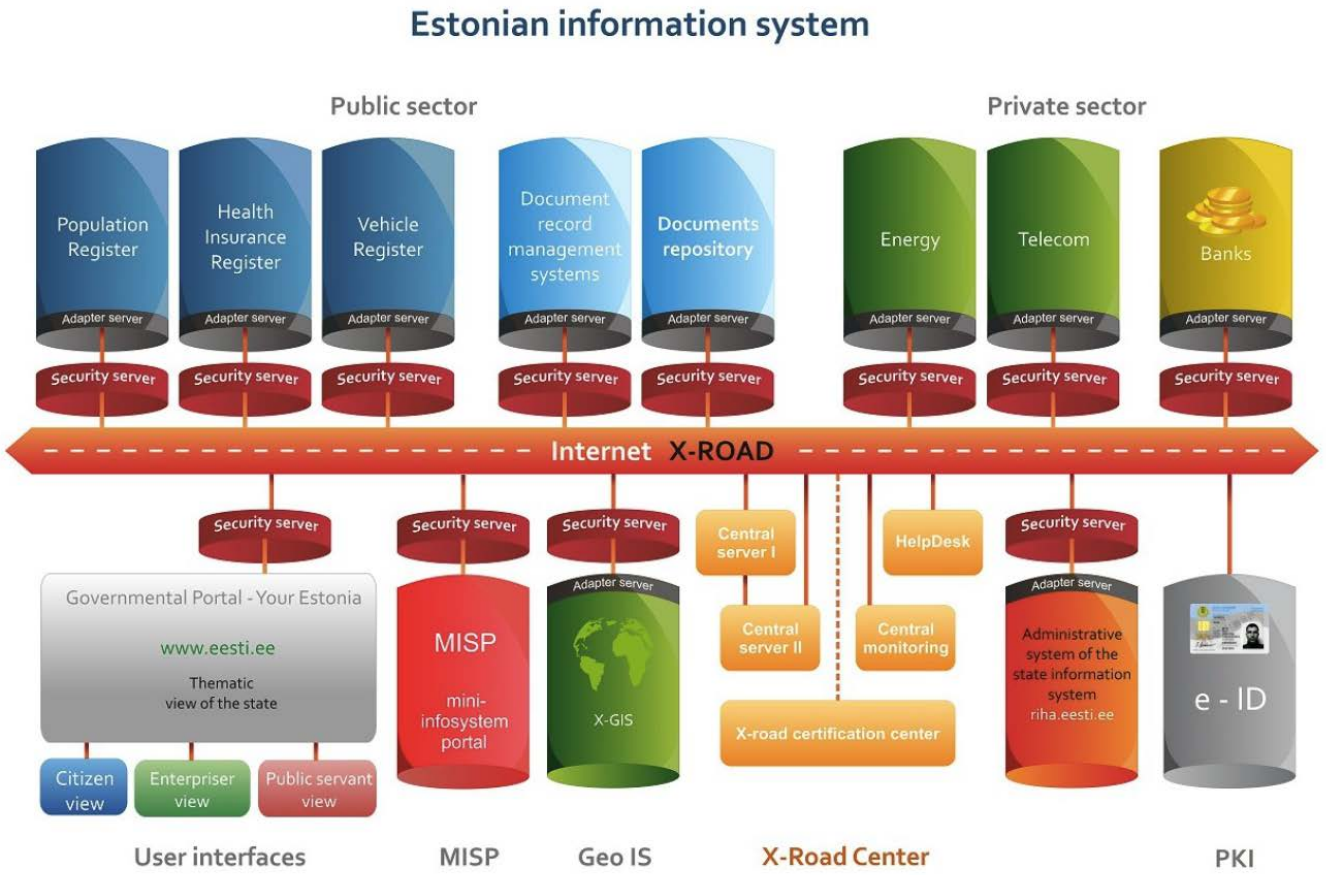
# Cross-sector e-strategies: Examples of ITU experiences




e-Agriculture Strategy Guide

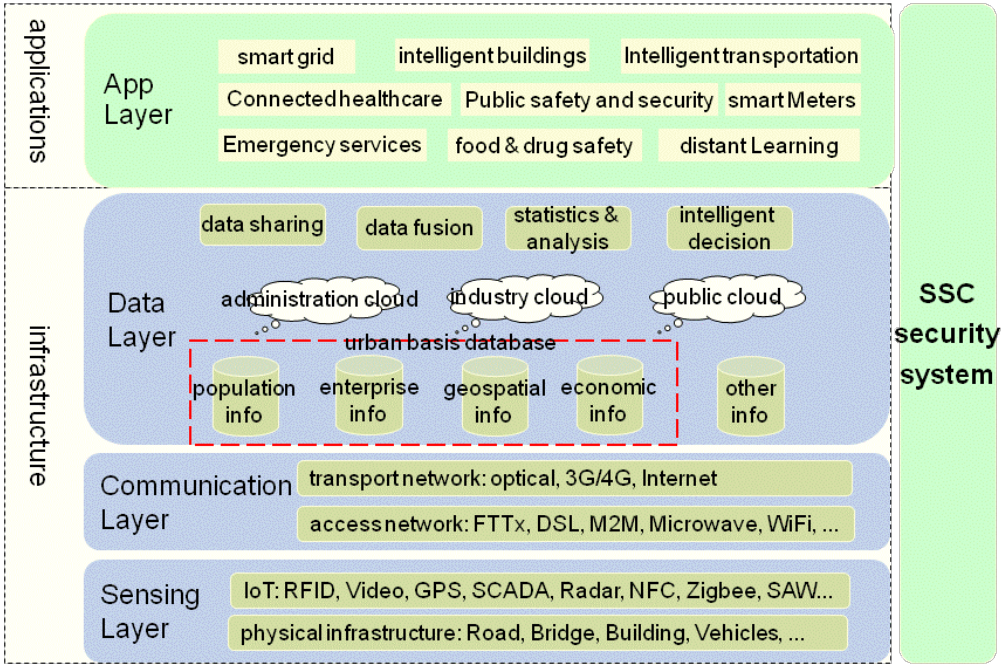
Implementing e-strategies requires some common requirements e.g. Cloud, Security, Privacy, Sensors, Big Data Analysis, Interoperability, Open Data, Applications Development, Digital Literacy etc.

# Example Estonia




Source: https://www.ria.ee/public/x_tee/xRoadOverview.pdf/

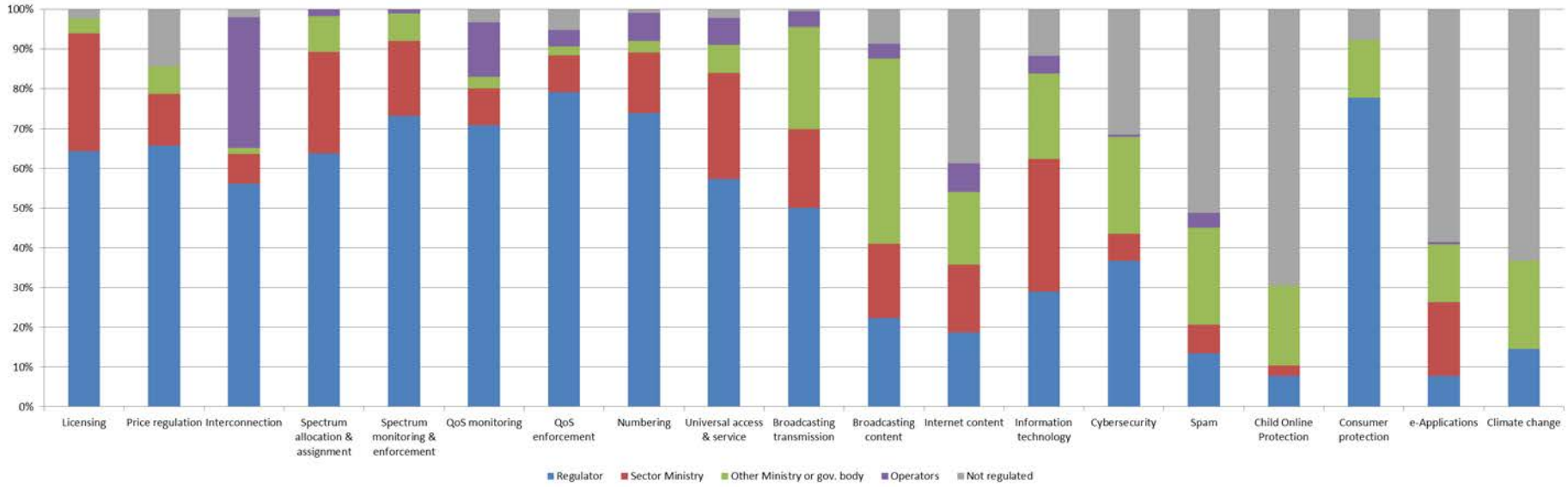

# Technical Architecture of a Smart Sustainable City




Telecom/ ICT Sector Issues (examples)

- Cross-Sector Collaboration
- Competition
- Investment
- Licensing
- Spectrum
- HetNets
- Broadband
- Cloud
- IoT / M2M
- Interoperability
- QoS/QoE
- Numbering & Addressing
- Big Data & Open Data
- Security
- Privacy
- Right of Way
- Infrastructure Sharing
- Green ICTs
- Data Centres
- e-Waste
- Emergency Telecommunications

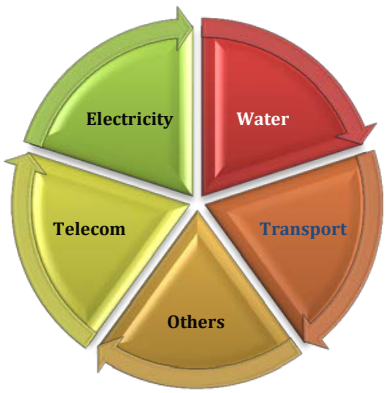
# Regulatory Mandate, 2013




Source: ITU World Telecommunication Regulatory Database

SMART SUSTAINABLE CITIES

# REGULATORY COLLABORATION




MULTI UTILITY REGULATOR

# Collaboration Mechanisms


Emergency


Education


Health


Electricity

Governance


Transport, Trade, Logistics

- Integrated Policy
- Legislation
- Co-Regulation
- Standardization (International / National)
- MoU or Cooperation Agreement
- Coordination Committee
- Projects, Coordination on Case to Case basis


Water


Teleworking


Infrastructure Security

# Collaboration Examples

Mobile Banking

| | |
|---|---|
| Tanzania | **MoU** signed between Bank of Tanzania (BoT) and Tanzania Communication Regulatory Authority (TCRA). |
| India | Statutory guidelines for operationalizing M-Banking issued by the Reserve bank of India (RBI) for banks and Regulations by the Telecom Regulatory Authority of India **(TRAI)** on QoS, Tariffs for service providers. |
| Pakistan | **MoU** between Pakistan Telecommunication Authority **(PTA)** and State Bank of Pakistan (SBP) |

Competition

| | |
|---|---|
| Australia | Legislation separates powers between Australian Consumers and Competition Commission (ACCC) and Australian Communications and Media Authority (**ACMA**). Chairman of ACCC and ACMA are **Associate Members** in **ACMA** and ACCC respectively. |
| Mauritius | **MoU** Signed between Competition Commission (CCM) and **ICT Authority (ICTA)** |
| United Kingdom | **Agreement on procedures** between Office of Fair Trade (OFT) and Office of Communications **(OFCOM).** |

Green ICT & E-Waste

| | |
|---|---|
| Egypt | Green ICT Strategy implemented through a **MoU** between **Ministry of Communications & IT (MCIT)** and Ministry of Environmental Affairs (MEA) |
| Singapore | E2PO is a **multi-agency committee** led by the National Environment Agency (NEA) and the Energy Market Authority (EMA) and comprises the Economic Development Board (EDB), Land Transport Authority (LTA), Building and Construction Authority (BCA), Housing and Development Board (HDB), **Infocomm Authority of Singapore (IDA)**, Agency for Science, technology and Research (A*STAR), Urban Redevelopment Authority (URA), Jurong Town Corporation (JTC) and National Research Foundation (NRF). The Ministry of the Environment and Water Resources (MEWR) and Ministry of Trade and Industry (MTI) are also represented in the committee. |

# Collaboration Examples

**Health**

| | |
|---|---|
| Singapore | **Joint project** on Tele-health by Ministry of Health and Infocomm Development Authority **(IDA)** |
| United States | Joint Statement and **MoU** between Federal Communications Commission **(FCC)** and Food and Drug Administration (FDA) on broadband and wireless enabled medical devices |

**Electricity**

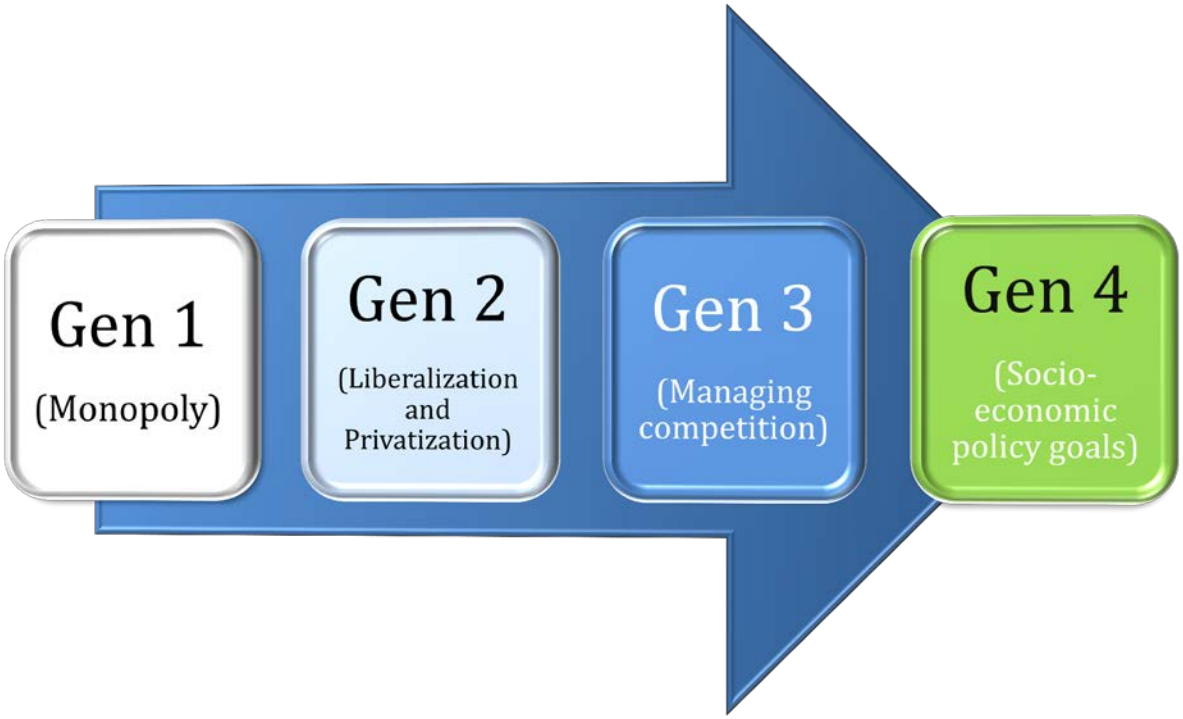
| | |
|---|---|
| Thailand | MoU between National Broadcasting and Telecommunications Commission (NBTC) and the Electricity Generating Authority of Thailand (EGAT) |
| UAE | Environment Agency - Abu Dhabi (EAD) and the **Telecommunications Regulatory Authority (TRA)** have signed a Memorandum of Understanding (**MoU**) to promote cooperation and partnership in the field of technology and information security, |

**Transport, Trade, Logistics**

| | |
|---|---|
| Singapore | Infocomm@SeaPort programme is a collaboration between the Infocomm Development Authority of Singapore **(IDA)** and the Maritime and Port Authority of Singapore (MPA). e-freight is a **joint programme** between IDA and Civil Aviation Authority of Singapore seeking to enhance competitiveness and increase productivity in the air cargo logistics sector through infocomm. |

**UK Regulators' Network (UKRN) is an initiative of the UK economic regulators: CAA, FCA, Ofcom Ofgem, ORR, Ofwat, UR. Monitor and the Water Industry Commission for Scotland (WICS) are also participating as observers**

# Regulation 4.0 - GSR 13 Best Practices

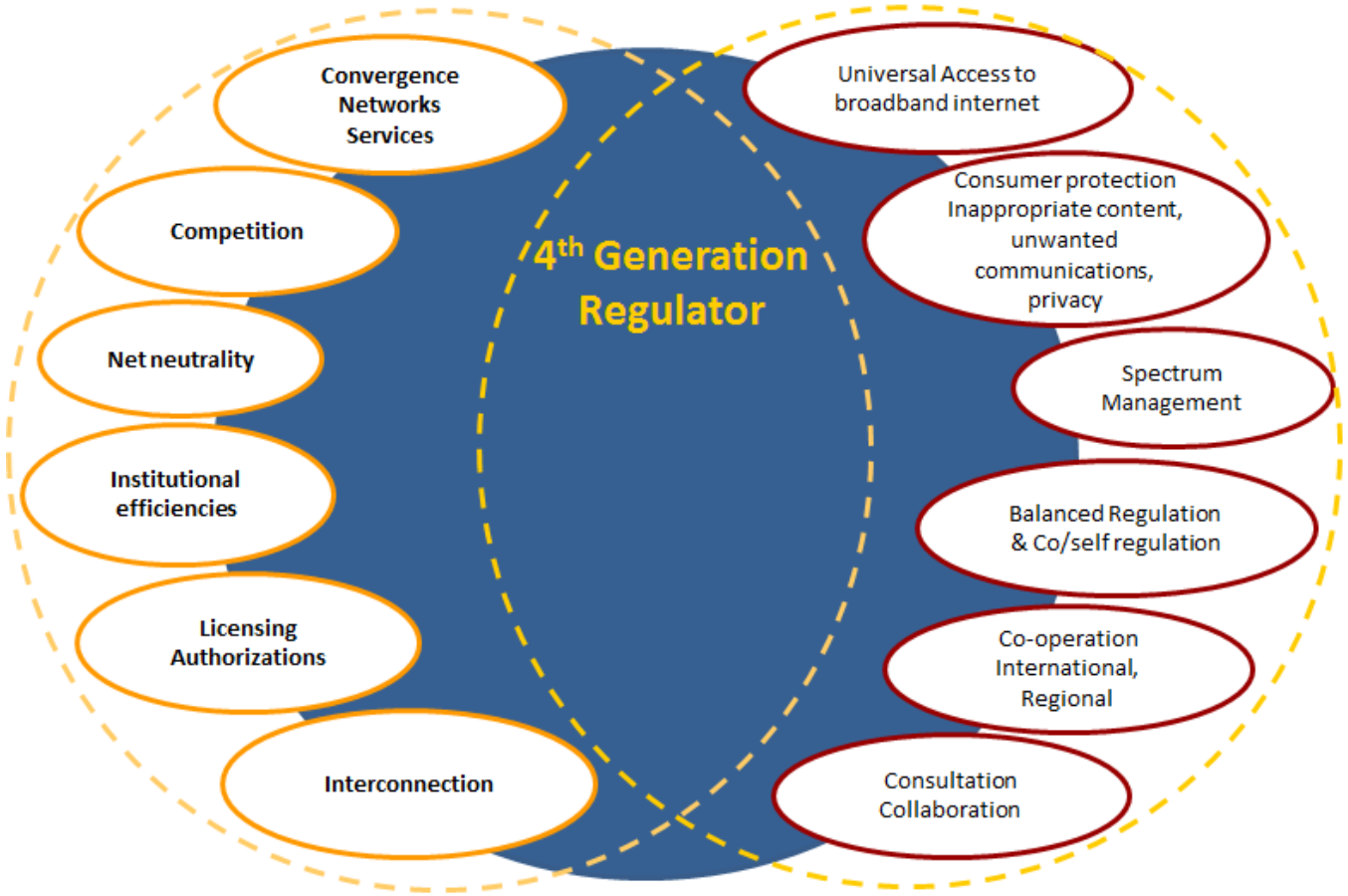



**1** Innovative and smart regulatory approaches fostering equal treatment of market players without putting extra burden on operators and service providers

**2** The evolving role of the regulator: the regulator as a partner for development and social inclusion

**3** The need to adapt the structure and institutional design of the regulator to develop future regulation

# Regulation 4.0




# Singapore Consultation (1/3)

**infocomm media in 2025**
Consultation Booklet
smart nation | innovative talent & enterprises | better living

**We are developing a Masterplan that will be released in 2015 to guide our infocomm and media sectors up to 2025. We will focus on:**

**5 STRATEGIC AREAS**

- ICM Infrastructure
- ICM Enterprise and Industry Development
- ICM Talent and Manpower Development
- Economic and Social Transformation
- ICM Technology and R&D

We envision Singapore as a Smart Nation where there is:

- Creative and effective use of technologies
- Connectivity anytime, anywhere, on any device
- Data protection and cybersecurity
- Better productivity
- Creation of new revenue streams
- Better informed government policy making
- Resilient ICM infrastructure

With Innovative Talent & Enterprises that:

- Thrive on culture of creating and building
- Create revolutionary ICM products and services
- Make compelling and inspiring content
- Produce innovative solutions

Where there is Better Living for all Singaporeans with:

- Improved ways for us to live, work and contribute to the building of a connected, cohesive and resilient community

Here are some preliminary ideas which are being considered for the Masterplan that will be released in 2015.
We invite you to share your views on them with us.

| Strategies | Ideas |
|---|---|
| Establish agile, pervasive and trusted ICM infrastructure | . Heterogeneous Network<br>. Above Ground Box<br>. Digital Harbour<br>. Data Marketplace |
| Build vibrant, strategic and enabled ICM sectors | . Self-Sustaining Start-up Ecosystem<br>. Media Service for Next Generation Seniors |
| Develop and retain passionate ICM human capital with relevant skills | . Computational Thinking as a National Capability<br>. Open and Accelerated Professional Development |
| Enable people and businesses to harness the power of ICM | . Smart Health-Assist<br>. Urban Logistics<br>. Community Time Exchange |
| Build a R&D ecosystem that supports ICM innovation and commercialisation | . Fast and Affordable IP Licensing Framework<br>. Enhance Market Demand for ICM Technologies |

We want to contribute towards a Better Quality of Life for Singaporeans with innovative ICM solutions that support the way Singaporeans work, live and play. We want Sustainable and Quality Growth using the ICM sectors to optimise our national resources, drive productivity for critical industries, and build globally competitive Singapore-based ICM companies.


Source: http://www.mci.gov.sg/web/content/infocomm-media-masterplan

# Singapore Consultation (2/3)

**infocomm media** in 2025

Consultation Booklet

smart nation | innovative talent & enterprises | better living

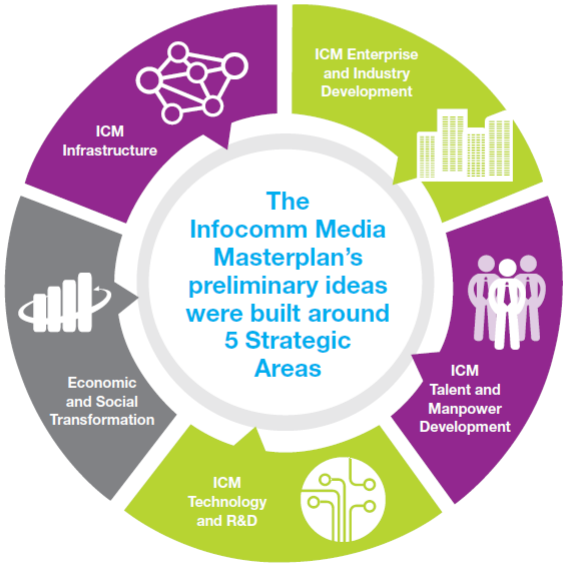

## The Consultation Process: We Sought Your Views

**On 31 March 2014, the Infocomm Media Masterplan Steering Committee released a consultation document for the Infocomm Media Masterplan.**

**This document:**

- Outlined the vision for Singapore's infocomm and media (ICM) sectors until 2025[1]; and
- Described 13 preliminary ideas for the Masterplan. The ideas are built around five strategic areas aimed at ensuring a better quality of life for Singaporeans and sustained growth for Singapore.

The consultation process for the Masterplan is now completed. This booklet highlights feedback gathered during this part of the consultation process.




## How Can The Infocomm Media Masterplan Best Meet Your Aspirations?

Your suggestions on how the Masterplan can best meet your aspirations:

1

**By Building Capabilities and Infrastructure and Growing Local Enterprises**

**This includes:**

- creating an environment where local firms and start-ups can thrive, and
- promoting alternate funding avenues for local firms (in addition to Government grants).
- training local infocomm and media (ICM) talent,
- making internet connection costs more affordable.

2

**By Capitalising on Singapore as a Living Lab**

- We should capitalise on Singapore being an ideal testbed for innovative technologies by investing in R&D and commercialisation of technology to grow our industries and competitiveness.

3

**By Improving our Media and Content Creation Sectors**

- Stakeholders want more media ideas and more support for media professionals developing compelling and exportable content.

4

**By Focusing on Quality of Life**

- Beyond galvanising the economy, the Masterplan should improve the quality of life for all, especially that of seniors.

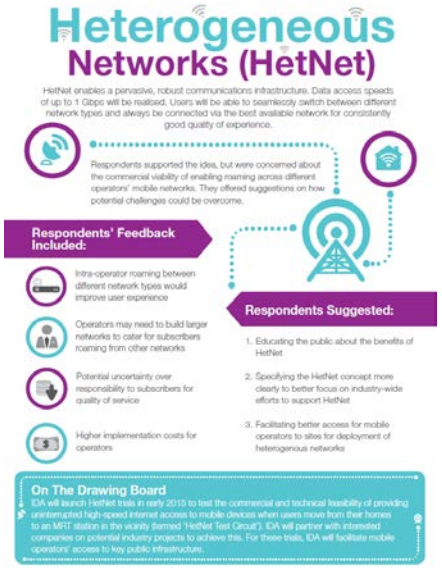
[1] The consultation document can be downloaded from http://www.mci.gov.sg/content/mci_corp/web/mci/infocomm_media_masterplan.html

**Source: http://www.mci.gov.sg/web/content/infocomm-media-masterplan**

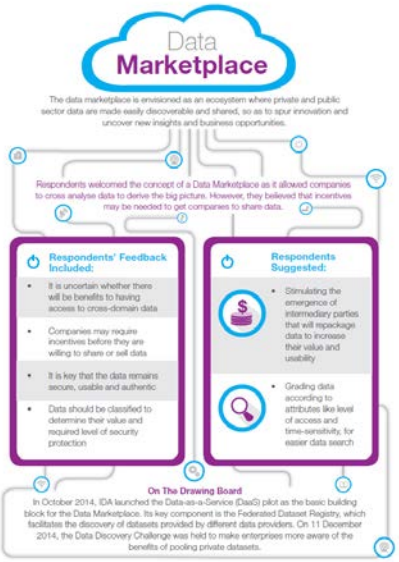
# Singapore Consultation (3/3)

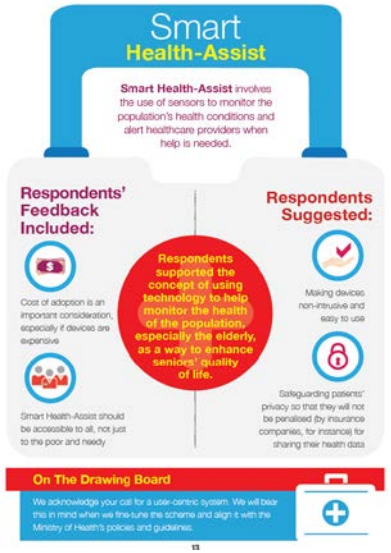
infocomm media in 2025
Consultation Booklet
smart nation | innovative talent & enterprises | better living

## Discussion Issues (Sample) ……








**For details, please visit http://www.mci.gov.sg/web/content/infocomm-media-masterplan**

# Machine to Machine Communication: Potential Frequency Bands

## IMT Bands (mainly for wide area M2M applications)

| Band (Mhz) | RR provisions identifying bands for IMT |
|---|---|
| 450-470 | 5.286AA |
| 698-960 | 5.313A, 5.317A |
| 1 710-2 025 | 5.384A, 5.388 |
| 2 110-2 200 | 5.388 |
| 2 300-2 400 | 5.384A |
| 2 500-2 690 | 5.384A |
| 3 400-3 600 | 5.430A, 5.432A, 5.432B, 5.433A |

**Also, frequencies identified by national administrations for short-range devices and allocated to fixed or mobile service**

## Commonly Used Frequency Ranges for Short Range Devices

**Commonly used frequency ranges**

| ISM within bands under RR Nos. 5.138 and 5.150 | |
|---|---|
| 6 765-6 795 kHz<br>13 553-13 567 kHz<br>26 957-27 283 kHz<br>40.66-40.70 MHz<br>2 400-2 483.5 MHz<br>5 725-5 875 MHz<br>24-24.25 GHz<br>61-61.5 GHz<br>122-123 GHz<br>244-246 GHz | |
| **Other commonly used frequency ranges** | |
| 9-135 kHz: | Commonly used for inductive short-range radiocommunication applications |
| 3 155-3 195 kHz: | Wireless hearing aids (RR No. 5.116) |
| 402-405 MHz: | Ultra low power active medical implants Recommendation ITU-R RS.1346 |
| 5 795-5 805 MHz: | Transport information and control systems Recommendation ITU-R M.1453 |
| 5 805-5 815 MHz: | Transport information and control systems Recommendation ITU-R M.1453 |
| 76-77 GHz: | Transport information and control system (radar) Recommendation ITU-R M.1452 |

NOTE 1 – See also Recommendation ITU-R SM.1756 – Framework for the introduction of devices using ultra-wideband technology.

Source: ITU-R Report SM.2153-4

# M2M application characteristics and their implications for spectrum

## A study by Aegis Systems Limited and Machina Research for OFCOM (U.K.)

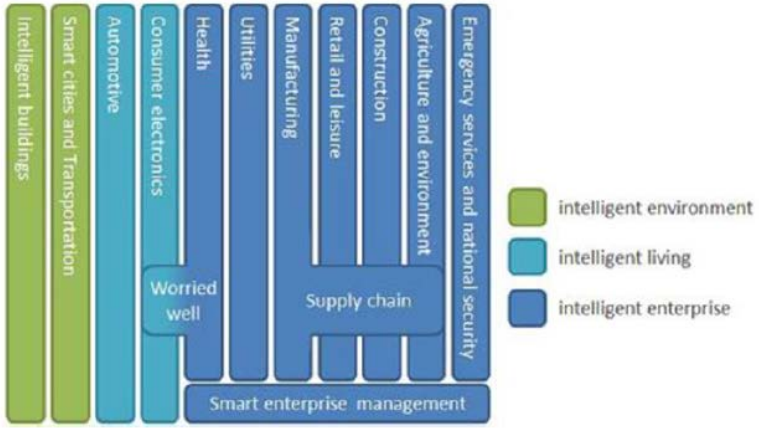



Figure 5-3: Final proposed set of M2M groupings

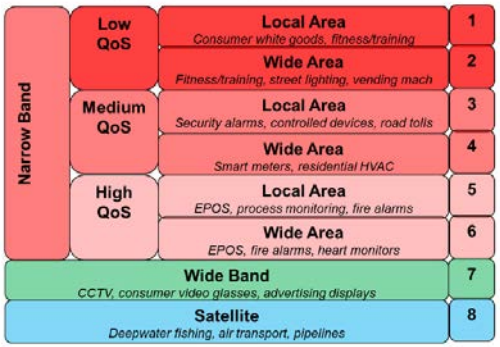



Figure 0-5 Distribution of Transactions by grouping

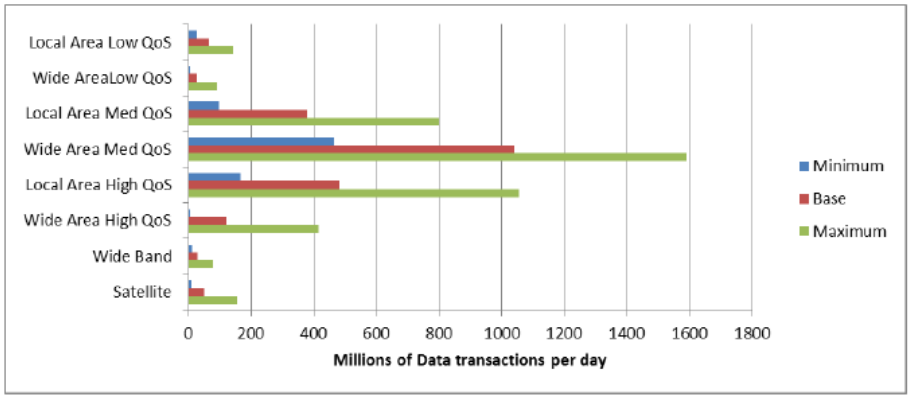
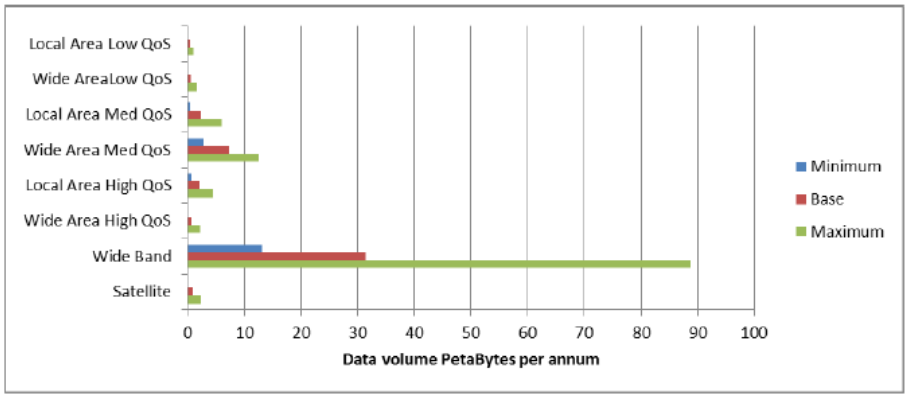



Figure 0-6 Distribution of Data volumes by grouping

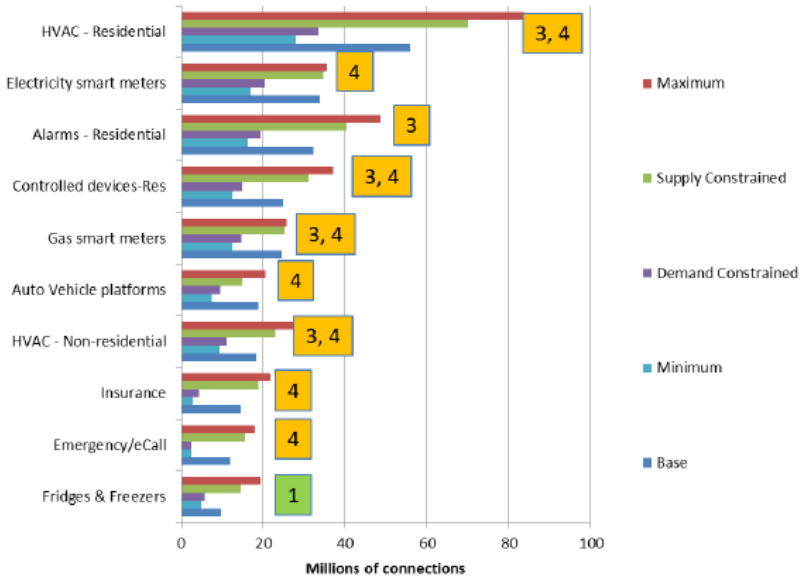



Source: http://stakeholders.ofcom.org.uk/market-data-research/other/technology-research/

# M2M application characteristics and their implications for spectrum

## A study by Aegis Systems Limited and Machina Research for OFCOM (U.K.)

Figure 0-7: Dominant applications in terms of number of daily data transactions




*"The volume of data generated by M2M applications is relatively small compared to the wider mobile data market – our estimates for 2022 lie in the range 20 to 65 petabytes per year which is likely to be less than one per cent of total cellular data traffic (and not all of this M2M data will be carried over cellular networks). However the number of connections are likely to exceed the number of other connected mobile data devices (our projections indicate between 170 and 530 million), and the number of data transactions generated is expected to be in excess of a billion per day.*

*If M2M applications continue to rely heavily on existing 2G or 3G cellular technology such transaction volumes could be problematic as these networks are not well suited to carrying large volumes of small data transactions, because each transaction can take a second or more to initiate and terminate, far more network resources are consumed then would be implied by the amount of data transmitted, ultimately leading to a need for either more infrastructure or more spectrum."*

Source: http://stakeholders.ofcom.org.uk/market-data-research/other/technology-research/

# IMT Spectrum Estimates

| RATG 1: Pre-IMT, IMT-2000 and its enhancements | RATG 2: IMT-Advanced (new mobile access and new nomadic/ local area access) | RATG 3: Existing radio LANs and their enhancements | RATG 4: Digital mobile broadcasting systems and their enhancements |
|---|---|---|---|

**Total spectrum requirements for both RATG 1 and RATG 2 in the year 2020**

| | Total spectrum requirements for RATG 1 | Total spectrum requirements for RATG 2 | Total spectrum requirements RATGs 1 and 2 |
|---|---|---|---|
| Lower user density settings | 440 MHz | 900 MHz | 1 340 MHz |
| Higher user density settings | 540 MHz | 1 420 MHz | 1 960 MHz |

- Source: Report ITU-R M.2290-0 (12/2013)

# Internet of Things (IOT) Standardization & Roadmap - ITU

***Internet of things (IoT)**: A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies.* - ITU-T Rec. Y. 2060

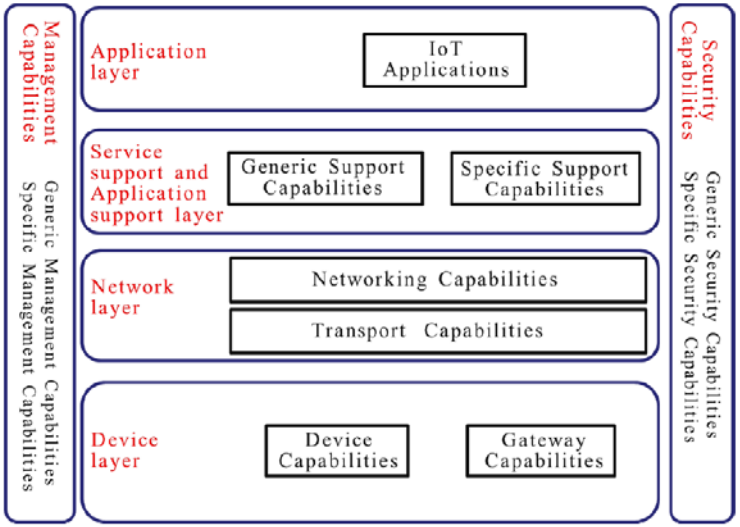



**Figure 4 – IoT reference model**

The ITU-T activities related to IoT expanded when TSAG established in 2011 the IoT Global Standards Initiative (IoT-GSI) as a consolidated working platform to progress IoT standardization in ITU-T. ITU-T produced Recommendations spanning an IoT framework (basic concepts and terminology, common requirements and capabilities, ecosystem and business models, etc.), various areas of applications and services (e.g. networked vehicles, e-health, home networks, machine-oriented communications, sensor control networks, gateway applications), as well as testing aspects.

The Joint coordination activity (JCA-IoT: http://itu.int/en/ITU-T/jca/iot) developed and maintains an " IoT Standards Roadmap", a cross-SDO list of IoT standard specifications.

ITU-T SG 5 created a new Question (Q20/5) on Smart Sustainable Cities and Communities.

ITU-T SG 13 (Future Networks), ITU-T SG-17 (Security), ITU-T SG 16 (Multimedia), Others

# Examples of e-waste policies worldwide

**ITU Connect 2020 Agenda:** roadmap for the ICT sector to meet

- Target 3.2: Volume of redundant e-waste to be reduced by 50% by 2020

Photo credit: thedailygreen.com

## European Union

- WEEE Directive (on e-waste)
- RoHS Directive (on hazardous substances)

## Costa Rica

- Electronic Waste Management, Decree No. 35933-S, 2010

Photo credit: Estre Ambiental/Handout www.worldbank.org

**People's Republic of China:** Decree No.551 of the State Council

- Regulations on the Management of the Recovery and Treatment of Waste Electronic and Electrical Products

A tonne of gold ore yields just 5 gms of gold, whereas a tonne of used mobile phones yields a staggering 400 gms.

# Open Data Examples

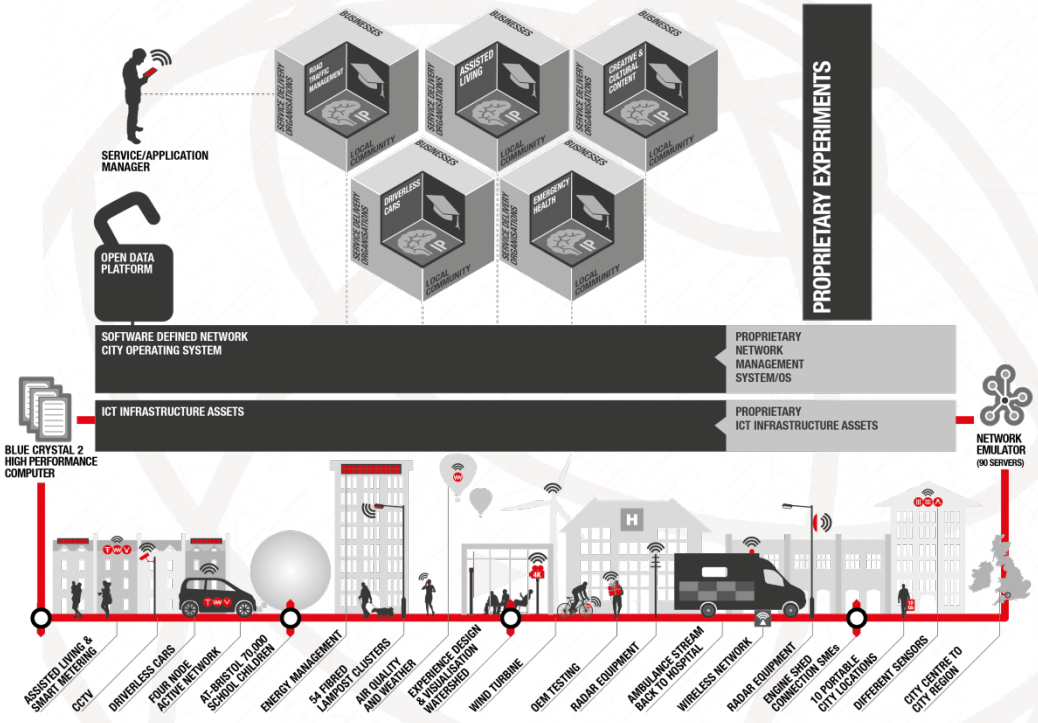



Figure Source: Presentation by Mr. Joe Dignan, Member of the Future Cities Department, Bristol City Council - "Bristol is open http://www.itu.int/en/ITU-T/Workshops-and-Seminars/Pages/201503/Programme.aspx

- Australia
http://www.ausgoal.gov.au/ausgoal-qualities-of-open-data

- New Zealand
https://ict.govt.nz/guidance-and-resources/open-government/new-zealand-data-and-information-management-principles/

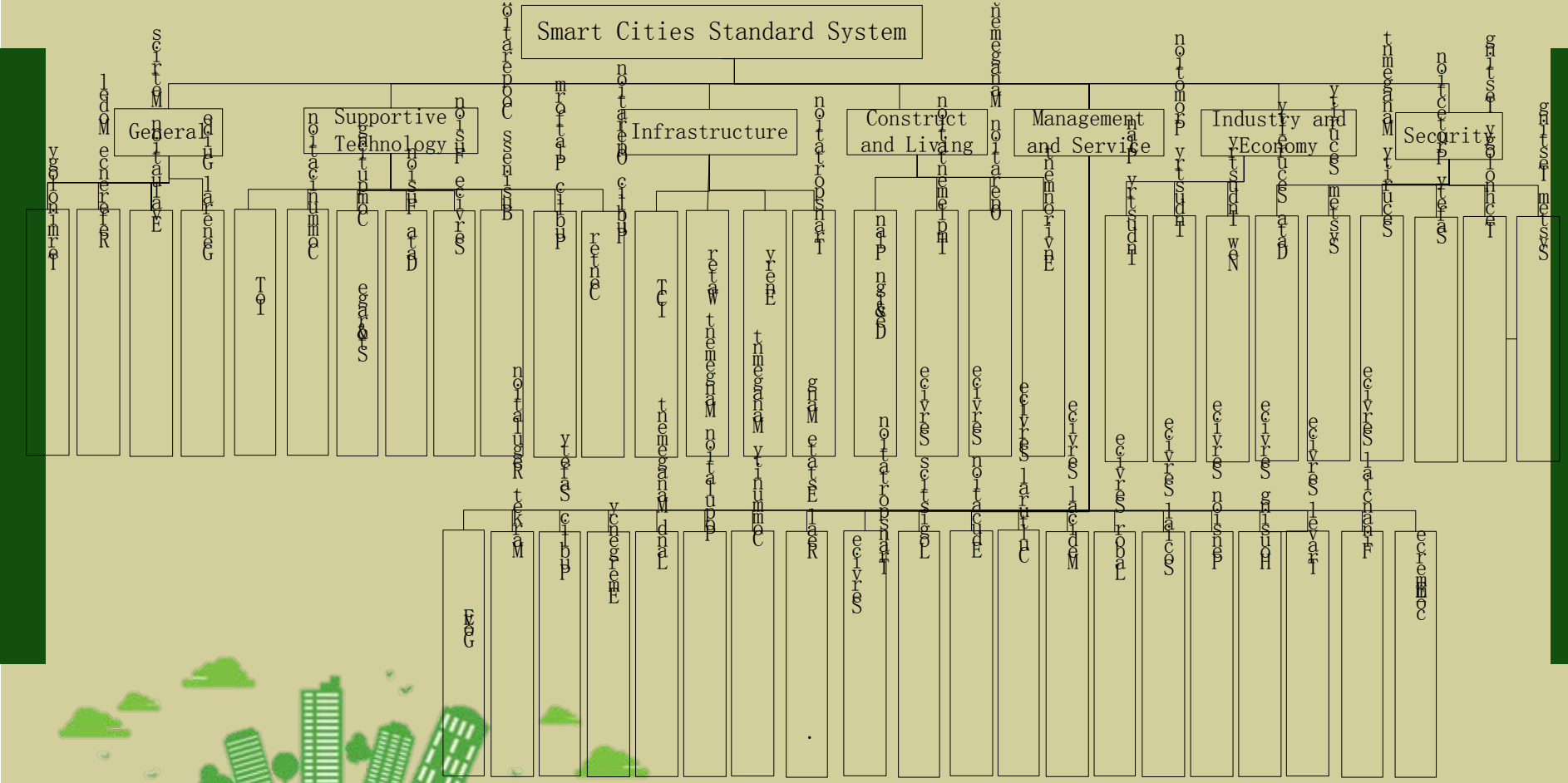
- Kitchener
http://www.kitchener.ca/en/insidecityhall/resources/FCS_Kitchener_OpenDataFrameworkIntroduction_Oct2313.pdf

- **United Kingdom**
http://Data.gov.uk

- **Singapore**
http://Data.gov.sg

# 初步规划了智慧城市标准体系
# Draft Smart Cities Standards System

China




*Source: Lei Zang, China Academy of Telecommunication Research (CATR), ITU Green Standards Week, 22-26 September 2014, Beijing*

# The SSC cyber-equation

- "Smart and Sustainable Cities" have ICT as key enabler
- This implies:
  - Highly complexity of the ICT systems
  - Highly interconnected components
  - High volume of data generated

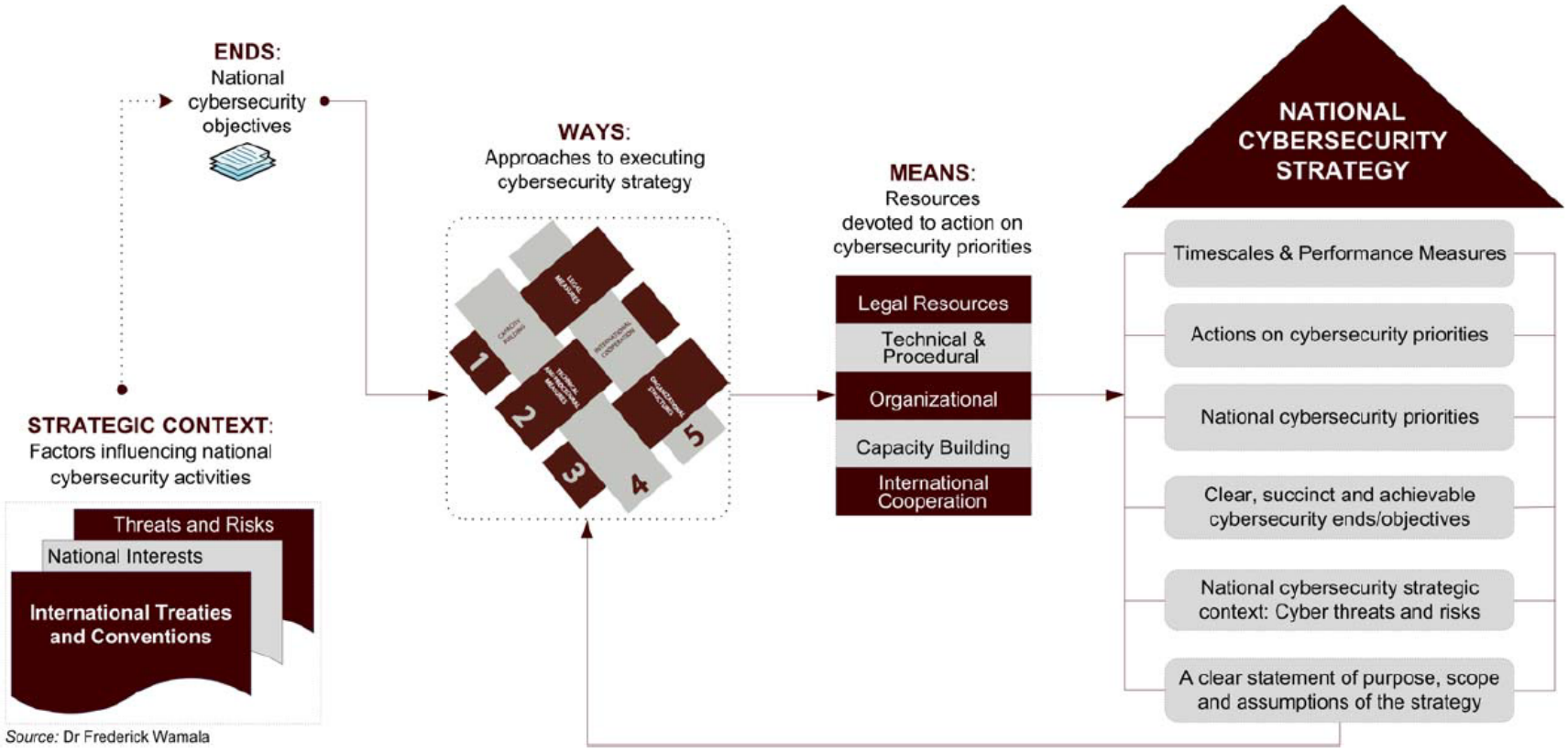

# A resilient Smart and Sustainable City…

…needs to be designed, from incepti
with…

- Cyber security
- Privacy
- Integrity
- Compliance
- Reliability
- Resilience

…in mind.

# National Cybersecurity Strategy




*Source:* Dr Frederick Wamala

# Technologies involved & vulnerabilities

- Network Infrastructure
- Cloud Computing (availability, security)
- Internet of Things (sensors, RFID, M2M, Standards…)
- Data and Big Data (embed security with data, confidentiality, integrity, authentication, availability)
- Legislation increasingly prescriptive,

# Ensuring continuity of critical services

- City governance to ensure that ICT strategies are strongly interwoven into the fabric of the wider city evolution strategy
- Technology to enable policy
- City CIOs increasingly part of strategic policy discussions
- Systems/IoT, need to be standardised, interoperable and open, but also secure
- Cyber-security and resilience to be embedded from inception
- Cyber-security + backup and recovery systems for mission-critical administration data (& Big Data)
- Legislation increasingly prescriptive

# Recommendations – Security & Resilience

- **Establish Governance -** Identify and organise key stakeholders
- **Governance, Risk and Compliance (GRC) -** Fulfil through policies and processes, enabled by *ad hoc* IT suites: stay compliant and mitigate risks
- **Service continuity** - Solutions and methodologies on Cyber-security, backup, data loss prevention, archiving and disaster recovery.
- **Protect information proactively**
  - Information-centric approach
  - Embed security within data
  - Utilise encryption
- **Authenticate users** with Strong Authentication
  - This also prevents from accidental disclosing of credentials and from attaching unauthorised devices to the infrastructure.

# Recommendations – Security & Resilience

- **Threat intelligence** - In order to understand the major trends in terms of potential attackers, through analysing trends on malware, security threats, and vulnerabilities
- **Managed security services** - Outsourcing security services to providers. The ICT leadership can in that way focus on their functional duties of running the city systems
- Rely on their national Computer Emergency Response Teams (CERT), in order to be aligned with national coordination on cyber-incidents and security, and benefit from the international visibility this provides these entities provide.
- **Protect the infrastructure** by securing endpoints, messaging and web environments.
- **Ensure 24x7 availability of the critical infrastructure**
- **Develop an information management strategy**

# Cloud computing security framework

The distributed and multi-tenant nature of cloud computing, the prevalence of remote access to cloud computing services and the number of entities involved in each process make cloud computing inherently more vulnerable to both internal and external security threats than other paradigms.

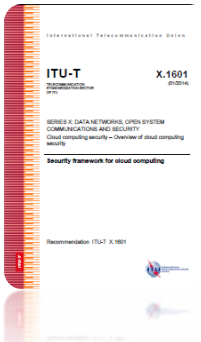
## Security threats

(associated with attacks (both active and passive), and also environmental failures or disasters)

## Security challenges

(comprise difficulties arising from the nature and operating environment of cloud services. When not properly addressed, security challenges may leave doors open for threats)

High-level security capabilities




# Cloud computing security framework

Step 1: Identify security threats and security implications of the challenges in the cloud computing service under study.

Step 2: Identify the needed high-level security capabilities based on identified threats and challenges which could mitigate security threats and address security challenges.

Step 3: Derive security controls, policies and procedures which could provide the security abilities that are needed based on identified security capabilities

## Security threats

(associated with attacks (both active and passive), and also environmental failures or disasters)

## Security challenges

(comprise difficulties arising from the nature and operating environment of cloud services. When not properly addressed, security challenges may leave doors open for threats)

High-level security capabilities

Security controls, policies and procedures

# Example: Mapping of cloud computing security threats and challenges to security capabilities I

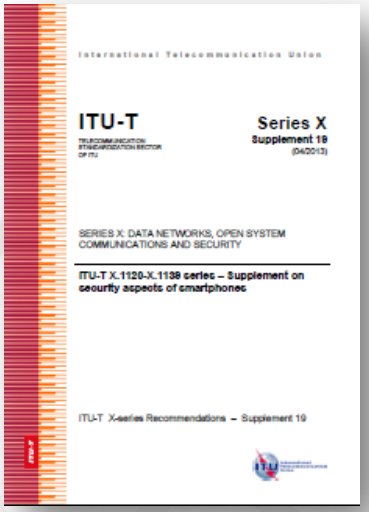
**Table I.1 – Mapping of cloud computing security threats and challenges to security capabilities**

| | | | Clause 9 Cloud computing security capabilities | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | Clause9.1 Trust model | Clause 9.2 Identity and access management (IAM), authentication, authorization and transaction audit | Clause 9.3 Physical security | Clause 9.4 Interface security | Clause 9.5 Computing virtualization security | Clause 9.6 Network security | Clause 9.7 Data isolation, protection and privacy protection | Clause 9.8 Security coordination | Clause 9.9 Operational security | Clause 9.10 Incident management | Clause 9.11 Disaster recovery | Clause 9.12 Service security assessment and audit | Clause 9.13 Interoperability, portability and reversibility | Clause 9.14 Supply chain security |
| Clause 7 Security threats for cloud computing | Clause 7.1 Security threats for cloud service customers (CSCs) | Clause 7.1.1 Data loss and leakage | Y | Y | Y | | | | Y | | | | Y | | | |
| | | Clause 7.1.2 Insecure service access | Y | Y | | Y | Y | Y | | | | | | | | |
| | | Clause 7.1.3 Insider threats | | Y | Y | | | | | | | | | Y | | |
| | Clause 7.2 Security threats for cloud service providers (CSPs) | Clause 7.2.1 Unautho-rized administra-tion access | Y | Y | Y | Y | | | | | | | | | | |
| | | Clause 7.2.2 Insider threats | | Y | Y | | | | | | | | | Y | | |

# Mapping of cloud computing security threats and challenges to security capabilities II

| | | | Clause 9 Cloud computing security capabilities | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | Clause9.1 Trust model | Clause 9.2 Identity and access management (IAM), authentication, authorization and transaction audit | Clause 9.3 Physical security | Clause 9.4 Interface security | Clause 9.5 Computing virtualization security | Clause 9.6 Network security | Clause 9.7 Data isolation, protection and privacy protection | Clause 9.8 Security coordination | Clause 9.9 Operational security | Clause 9.10 Incident management | Clause 9.11 Disaster recovery | Clause 9.12 Service security assessment and audit | Clause 9.13 Interoperability, portability and reversibility | Clause 9.14 Supply chain security |
| Clause 8 Security challenges for cloud computing | Clause 8.1 Security challenges for cloud service customers (CSCs) | Clause 8.1.1 Ambiguity in responsibility | | Y | | | | | | | Y | | | | | |
| | | Clause 8.1.2 Loss of trust | Y | | | | | | | | | | | Y | | |
| | | Clause 8.1.3 Loss of governance | | Y | Y | | | | Y | | Y | Y | Y | Y | | |
| | | Clause 8.1.4 Loss of privacy | | Y | | | | | Y | | | | | Y | | |
| | | Clause 8.1.5 Service unavailability | | | | | | | | Y | Y | Y | Y | | | Y |
| | | Clause 8.1.6 Cloud service provider lock-in | | | | | | | | | | | | | Y | |
| | | Clause 8.1.7 Misappropriation of intellectual property | | Y | Y | | | | Y | | Y | | | | | |
| | | Clause 8.1.8 Loss of software integrity | | Y | | | Y | | Y | | | | | | | |

# Smartphone Security



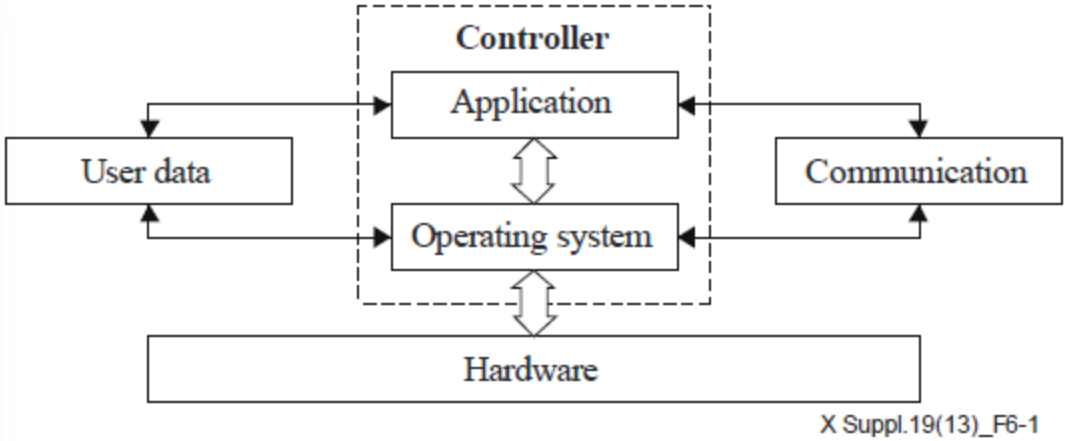
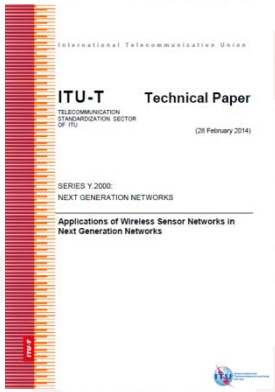




**Figure 6-1 – Common architecture of smartphones**

| Assets | Description | Importance |
|---|---|---|
| user data | Address book, call history, SMS/MMS, e-mail, pictures, audio, banking information, location information, notebook, agenda, etc. | Very important |
| software | Pre-installed applications, user-installed applications, operating system, etc. | Important |
| hardware | Central processing unit (CPU), random access memory (RAM), flash, battery, etc. | Important |

# Sensor Network Security




**Threats in sensor networks**

- **Vulnerability of sensor nodes;**
- **Eavesdropping ;**
- **Secrecy of sensed data;**
- **DoS attacks;**
- **Malicious use of commodity networks;**
- **Routing-specific threats**

In 2007 TSAG of ITU-T proposed to start work on this subject. Study Group 17 supported this proposal and created three work items covering USN security:

1. X.1311: Information technology – Security framework for Ubiquitous Sensor Networks
2. X.1312: Ubiquitous Sensor Network middleware security guidelines,
3. X.1313: Security requirements for wireless sensor network routing.


Appropriate and timely ICT policy & regulatory framework is very important for Smart Sustainable Cities……..