COSI – partnerships for Consumer Online Safety for the Internet

5th June 2009 – Download Version

Intercai Mondiale
Regatta House
High Street
Marlow
Buckinghamshire SL7 1AB

+44 (0) 1628 478470

www.intercai.co.uk

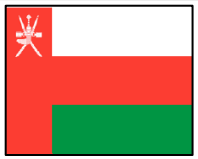
Contents

- Background
- Consumer On-line Safety for the Internet
- Forum Formation
- Content Rating National Hotline
- Forum Funding
- Forum Promotion
- Capability and Capacity Plans
- Audit and Enforcement

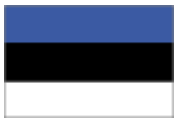
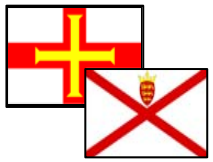
"Intercai Mondiale - The Business of Telecoms"

- Truly supplier independent
- Significant operator experience/expertise complementary to LEA expertise
- Track record of working in Oman, with TRA
- International Experience
  - Europe – Development of Content Filtering for Interception and Blocking for triple play operating businesses within Europe for a Global Operator
  - UK – Thought partner of Policy with the regulator for media and telecoms
  - UK – Due Diligence performed for a Venture Company upon a company providing multi-gigabit network encryption products globally
  - UK – Provision of Advisory Services for Skynet 5 military and commercial satellite voice and data services globally with international links
- Middle East Experience
  - Bahrain – Development of WiMAX infrastructure with network protection and key recovery to support Legal Interception
  - Jordan – Trust and Confidence Policy for E-Commerce through the use of PKI with a Certificate Authority
  - Kingdom of Saudi Arabia – Development of new entrant Mobile Network Operator(s) including Lawful Interception for Voice and Data traffic requirements
  - Kuwait - Development of Mobile Network Operator with Lawful Interception including Voice and Data traffic

Intercai's breadth of international experience






- Technology evaluation and policy
- Network Architecture & design
- Network/Services Quality
- Network Performance & Optimisation
- Content Management
- Business planning and technical support
- Technical and financial due diligence
- Sector policy and establishment of Regulator
- Licensing policy and licence award








Bio of Presenter - Angus Goldfinch

- Angus has had an extensive career involving policy and regulation for Mobile, Satellite and Fixed networks along with design and integration for security for IT and Telecommunications industries with a focus on network technologies, the applications running upon them and the integration with customer applications. He has worked closely with government agencies, telecom regulators, operators, enterprises and manufacturers.
- He is an expert of wireless and wireline networks with security, including voice, technology and its application for solutions in today's fast moving business environment. Angus has a proven track record in implementing Mobile, IP Telephony, Networks and Security for Small Medium and General Enterprise, Government and Telcos. His recent work includes regulation of Mobile, Value Added Services and software support systems for public safety and national security.

Background

- The realities of cyberspace make it clear that everyone has to work together.
- Responding effectively to cyber-threats requires resources, know-how and strong investments on capacity developments; these efforts cannot be undertaken by only one entity.
- The key element is bringing the public and the private sectors together in trusted forums and joint activities, to address the common cybersecurity challenges and develop solid capacity building plans.
- These collaborative efforts should involve every cyber-user; from citizens to corporations, law enforcement, and critical infrastructure providers.
- The basis of a successful partnership is trust, which is necessary for establishing, developing and maintaining sharing relationships between the different parties.
- This session looks closer at the benefits as well as challenges associated with innovative and sustainable partnerships for enhanced cybersecurity, and how joint efforts generate concrete steps forward.

Consumer On-line Safety for the Internet (COSI)

- Consumer On-line Safety for the Internet (COSI) requires the stakeholders in the public and private sectors to address the challenges against various threats to consumers, including but not limited to:
  - Content and child protection
  - Unsolicited commercial messaging (spam)
  - Scams (phishing and pharming)
  - Illegal downloading of music and film
  - …

COSI Stakeholders

- The stakeholders need to be brought together into a trusted forum undertaking activities together.
- This forum has to be built with new stakeholders that work with consumers using the existing partnerships, including but not limited to:
  - Child Welfare
  - Judiciary
  - Law Enforcement
  - Regulators
  - …

Existing Partnerships

- Suitable existing partnerships include but limited to:
  - National Security
    - » Telecom operators
    - » Corporations with their own telecommunications infrastructure,
    - » Telecom Regulator
    - » Concerned Agencies of National Governments
  - Public Safety
    - » Telecom operators
    - » Telecom Regulator
    - » Law Enforcement

Forum Formation

- The forum has to be clear in its purpose, operations model and its way forward, including but not limited to:
  - Aims of the association
    - » Obligations under law
    - » Obligations under regulations
    - » Obligations implied under licences
  - Preparation of principals and executive regulations
  - Defined reference model
  - Development of Code of Practice
  - Development of Framework
  - …

Forum has to deliver on its Aims

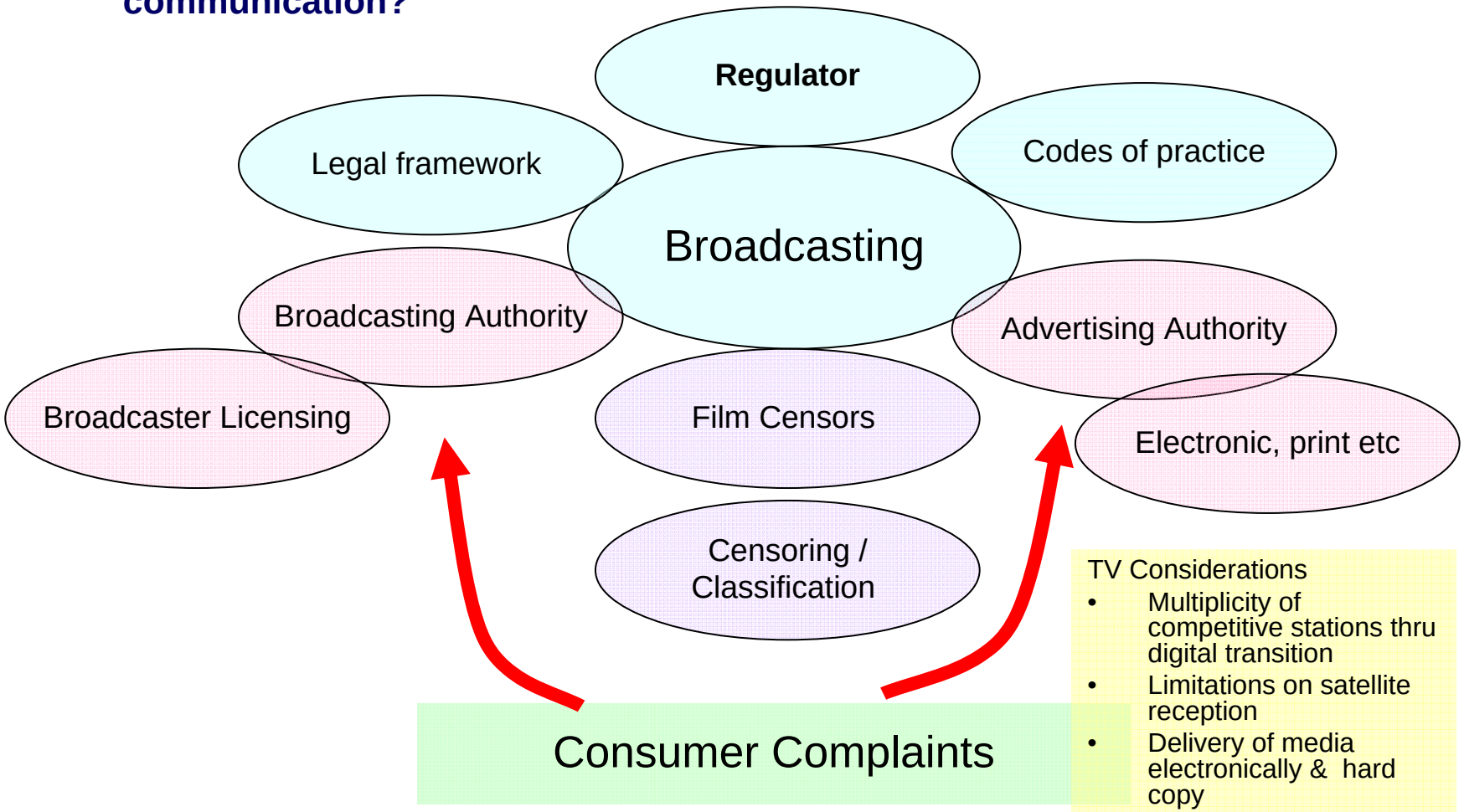
- The forum has to deliver against its aims. The aims have to be backed up through law or use of a number of laws. These laws themselves maybe supported with regulatory controls. The forum must be able to identify clearly a breach, audit it and enforce penalties against it by the relevant stakeholder(s)
  - Example applicable laws
    - » Data Protection
    - » Freedom of Information
    - » Freedom of Expression
    - » Intellectual Property
    - » ‘e-Transactions
    - » Consumer Protection
    - » Cyber Crime
    - » …
  - Example regulatory controls
    - » Crypto policy
    - » Data privacy
    - » Content filtering
    - » Traffic Analysis and Management
    - » Information Assurance
    - » Unsolicited Commercial Messaging
    - » IP Lawful Interception
    - » …

Content Rating National Hotline

- A key part of building the forum is the need for a national hotline to be setup allowing the public to report offending content:
  - Email
  - Web portal
  - Telephone
  - …
- The national hotline has to be able undertake content rating and validate the complaint.
  - The national hotline passes on for action to be undertaken by national stakeholders.
  - It maybe the offending content may not be within the country of the consumer making the report. The national hotline will then have to take up action with the hotline in the relevant country. It is necessary for the national hotline to develop links with hotlines in other countries and report upon it to the forum.

Broadcasting Practice

Broadcasting is the most established model of Content Regulation is. Does experience of this provide a model for regulation for other channels of communication?



TV Considerations

- Multiplicity of competitive stations thru digital transition
- Limitations on satellite reception
- Delivery of media electronically & hard copy

Broadcasting Regulatory Practice

- The requirement to introduce and enforce content regulation needs to be considered from a number of perspectives. If, for example, the regulatory model is too extensive, severe and granular, it may be unworkable and present an unmanageable responsibility on the regulator and also militate against socio economic objectives

- 'Best practice' in other countries uses different models for broadcasting and telecommunications. The latter, comprising internet and mobile, has different considerations because of the way in which infrastructure is managed where mobile has, for the moment, more formal controls.

The approach towards content regulation need to be set in the context of the

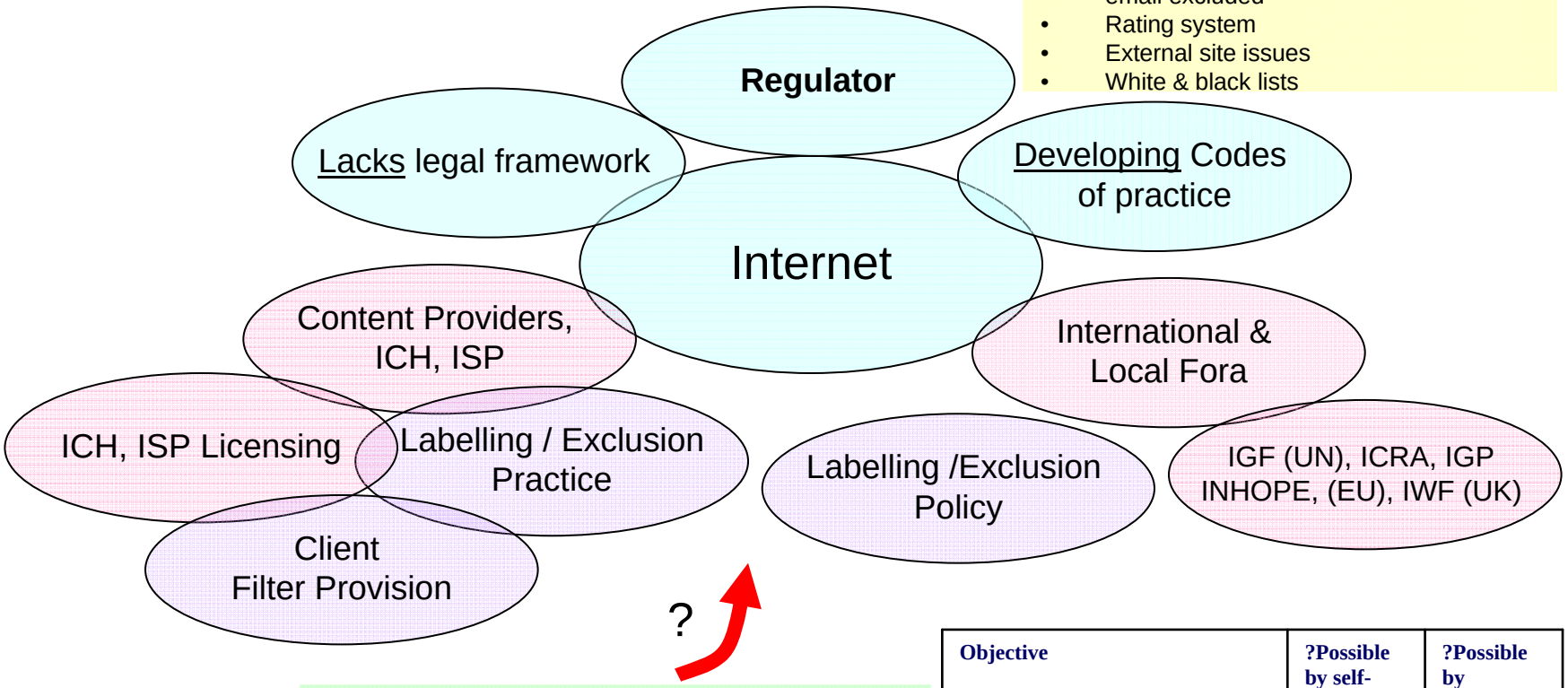
- The standards of the country and its culture
- Extent of regulation and the severity and granularity that is sought
- Proactive vs Reactive approach
- Regulatory models for the different types of media
- Regulatory mechanisms set in the context of a realistic expectation of compliance from third parties such as Service and Content Providers
- Required regulatory resources

Television Without Frontiers TWF

- European TWF Directive under debate
- Desire for EU single market in TV broadcasting and one that could compete with the USA with EU cultural and economic objectives
- TV only, not radio
- But TWF Directive is not technologically neutral. TV services via non-broadcast means are regulated differently to identical services that are broadcast.
- This is the nub of the matter that faces all in the new content space.

Internet Practice

- www, Usenet newsgroups, ...
- email excluded
- Rating system
- External site issues
- White & black lists



Objective Source: ICC	?Possible by self-regulation	?Possible by legislation
Enable adults to protect children from unsuitable material	Yes	No
Enable adults to control their own access to material they do not wish to see	Yes	No
Prevent communication of material which is illegal to possess	No	No

Consumer Education?

- Q? Should Content Regulation of Internet (practices and resources) be applied to Broadcasting and, if so, to what extent?

Mobile – Convergent Device?

- The mobile is becoming an access device where its use as a mobile phone for voice, messaging and multimedia services on the mobile operator's network represents its main but not sole function.
- Access to fixed lines is being introduced in the tariff war so that mobiles in range of the user's land line can have calls routed over the fixed infrastructure.
- With the increasing use of broadband coupled with the capability of mobile phones (internet/IP connectivity and web browsing) there is the prospect of these devices being used to access the web and related sites such as Usenet.
- The operator controlled model in the Walled Garden Scenario belies this internet / web access scenario.
- Matters to take into consideration are the uptake of mobiles (the overall range of devices) in young people and the issues of client protection software such as filtering and malware.
- Content regulation needs to take into account the way in which Mobiles may be used over the next 3 to 5 years and as Mobile Internet devices.

- For the purposes of content regulation, the mobile 'phone (inc PDA and other variants) should be viewed as an internet access device with the following attributes:
- predominant device for young people
- personal & therefore less parental control
- internet & web browsing functionality
- limited control re filtering & malware
- the need to look to future capabilities as well as considering those on the horizon

- Q? Should Content Regulation be considered from the perspective of convergence, ie all audio visual material that is communicated over IP?

MNO Practice

- **Setting the scene for Content Regulation internationally**
  - Should it aspire to be technology and platform neutral?
  - What is the level of pain and difficulty for the MNO?

Review of current practice

- Providing a review of practices of other countries
- All have come from a broadcasting regulation background
- They are seeking to address regulation of the internet, few are doing
- The mobile device represents the new wave of convergence
- Across Europe, no legislation is in place and codes of practice are used /
- MNOs have proclaimed their policy regarding their social responsibility
- MNOs have issued corporate responsibility statements and given timescales to the business to implement these.

Types of Content – many, varied and challenging

- TV
  - Programs
  - Film
  - Adverts
- Radio
  - Programs
  - Adverts
- Internet
  - www
  - Usenet newsgroups
  - FTP
- Mobile
  - MMS
  - Internet
  - all devices inc PDA

MNO Regulatory Status

- What is the MNO situation?
- What is the current level of content access control eg age verification, url filtering …. ?
- Is there a country code of practice and what is it?
- Is there a corporate responsibility statement and what is it?
- What are the timescales for implementation of the policy for each country operation?

Age Appropriate Content

Content Classification typically Culturally set

Age

10 11 12 13 14 15 16 17 18

UK

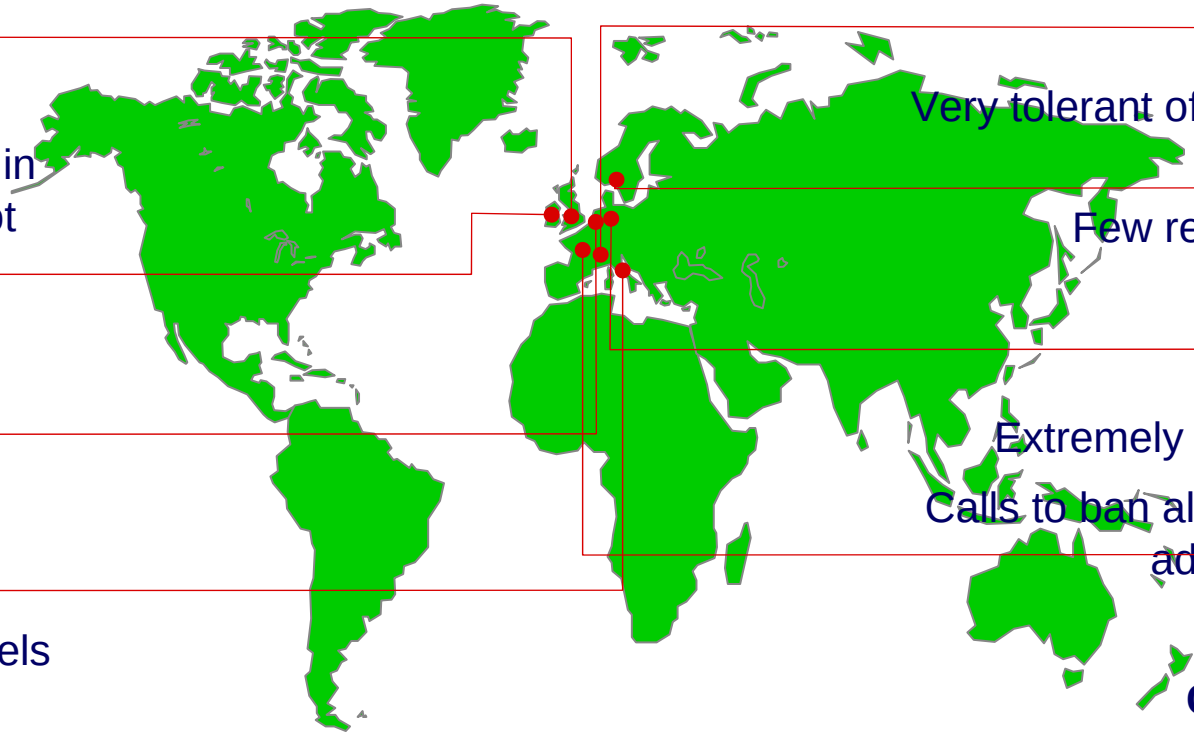
Canada

South America

Australia

Country Variances

Examples of local regulatory and social variances:



UK

Long tradition of topless modelling in the press – but not showing couples

Austria

Very tolerant of all erotic images

Few restrictions

Sweden

Extremely intolerant

Calls to ban all forms of adult media

Ireland

Nudity is not acceptable – not even topless models

Germany

High tolerance of erotic images, subject to proper minor protection controls

Netherlands

Very high level of tolerance to erotic images of all kinds

France

Individual Appropriate Content

Parental Specified Preferences

Individual Appropriate Content

- *Fashion Sites*
- *Friendship Sites*
- *Personalisation Sites*
- *Diet Sites*
- *Finance Sites*

Age Implication: Inbound Services

Age Verification also applies to in-bound services

- SMS / MMS Marketing
- Phishing (via SMS / MMS or Internet Links)
- Harassment / Nuisance Calls
- Inbound Chat
- Unknown originators
- Telemarketing (to minors)

Mobile – Recent European Developments

Policies of EU Telecoms and Justice Commissioners

- Mobile
  - Mobile Internet (Web and WAP)
    - » child protection in place banning illegal content
    - » Internet Watch Foundation (www.iwf.org.uk) black list used
    - » IWF works in conjunction with internet hot lines association inhope (www.inhope.org)
    - » STOP enforcement on materials for producing acts of terrorism
  - Mobile Business
    - » Tunnel traffic to Enterprise services to enforce corporate policies
    - » Using off the shelf products e.g. Blackberry
- Broadband
  - Consumer, Hot Spot & Hospitality Suite
    - » Similar to Mobile Internet
  - Business
    - » Similar to Mobile Business

Example Forum Funding Scheme

- Complaints about content are collected together into a black list for periodic validation, perhaps twice a day, that are distributed to stakeholders to use for referencing to bar access to this illegal content.
- Commercial stakeholders such as telecom operators are able to use it on their infrastructure to cleanse their services.
- This telecom operators could be paying members of the forum which they can use in their marketing to demonstrate support of cultural standards and social values
- The equipment vendors used by the telecom operators could be associate members paying for the ability to host the black list on their equipment

Forum National Promotion

- Its essential that the Forum is promoted to consumers and that they understand they are important, since they can provide details of illegal content to the national helpline.
- Ways of getting the message out about the forum include but are not limited to:
  - Roadshows
  - Free leaflets to hospitals, schools, universities, clubs…
  - Web sites of stakeholders
  - articles in the media
    - » newspapers, magazines, television progammes…
- This needs to be on a regular basis to describe purpose and provide success stories to encourage consumers to be active

Forum International Promotion

- We all understand that the Internet is global
- The Forum needs to be promoted to other national hotlines
- This allows for co-ordination between countries tackling threats to consumers safety from illegal content
- Policies maybe different between different countries i.e. one size does not fit all, and this needs to be understood in not just blocking access to content but requesting support in issuing of a take down notice to have content removed.
- For a take down noticed to be delivered against an illegal piece of content the national hotline of that country needs to initiate action

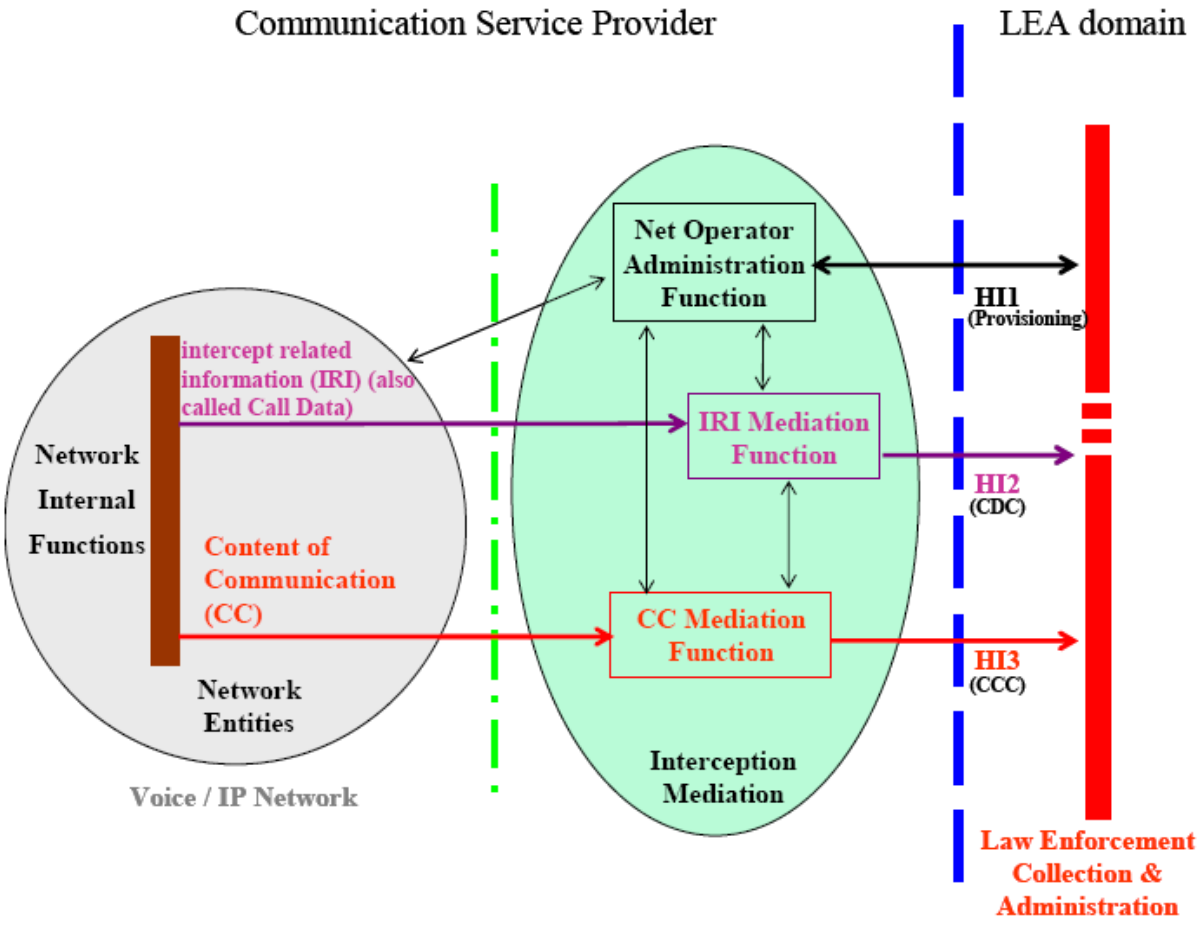
Capability and Capacity Plans

- The evolution of cybersecurity challenges requires solid capability and capacity plans with the existing partnerships for National Security and Public Safety to be developed and implemented, including but limited to:
  - Network Encryption
  - Lawful Interception
  - Data Retention
  - Malware
  - Information Assurance
  - Quality of Service

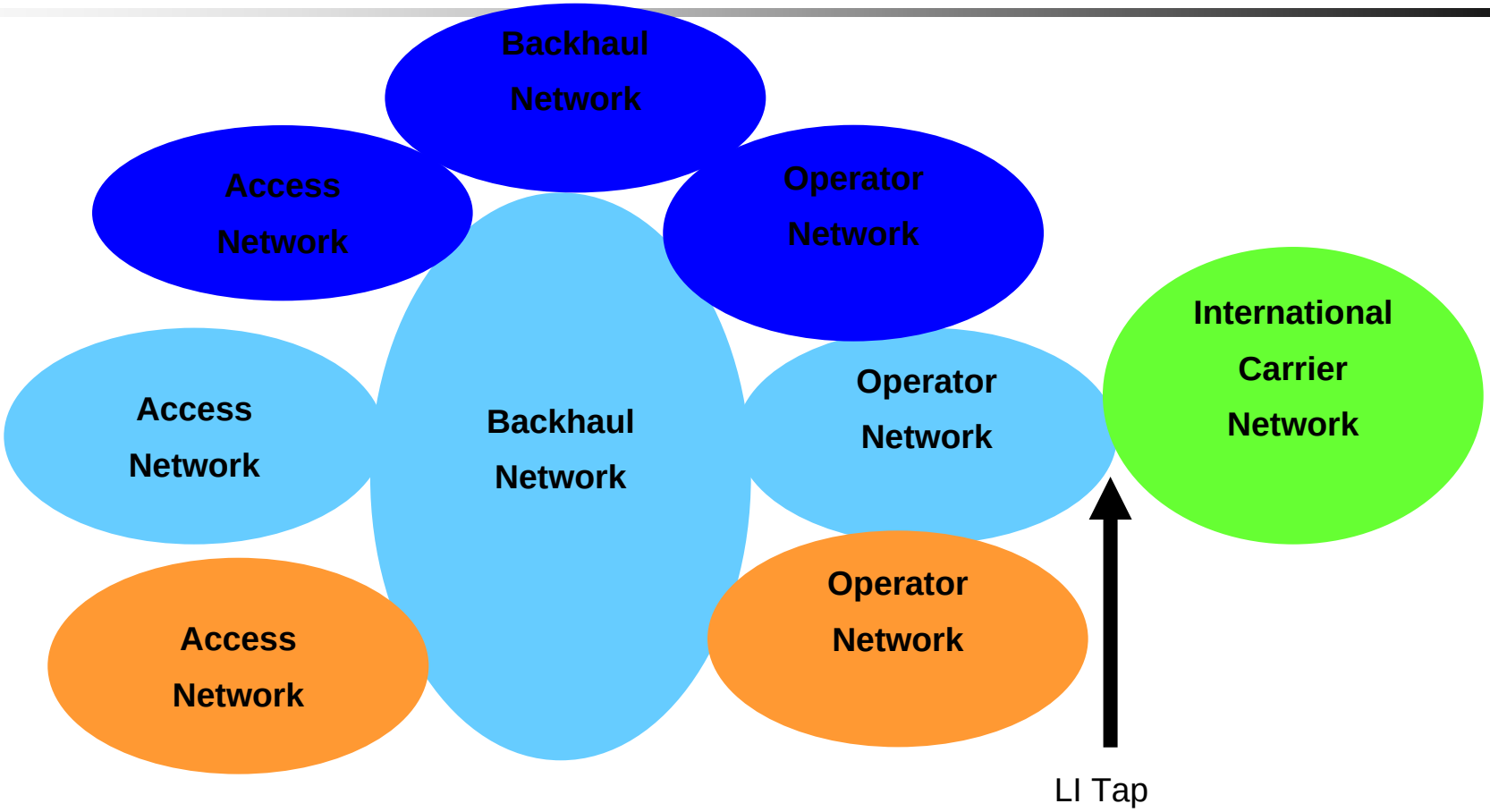
National Security for Liberalised Telecoms Market

- National Security Partnership has challenges in developing capacity and capability plans tracking telecoms market evolution
  - Government ownership
  - Incumbent based market
  - Liberalised telecoms market
    - » Access providers
    - » Service providers
    - » Network operators

ETSI LI Structure

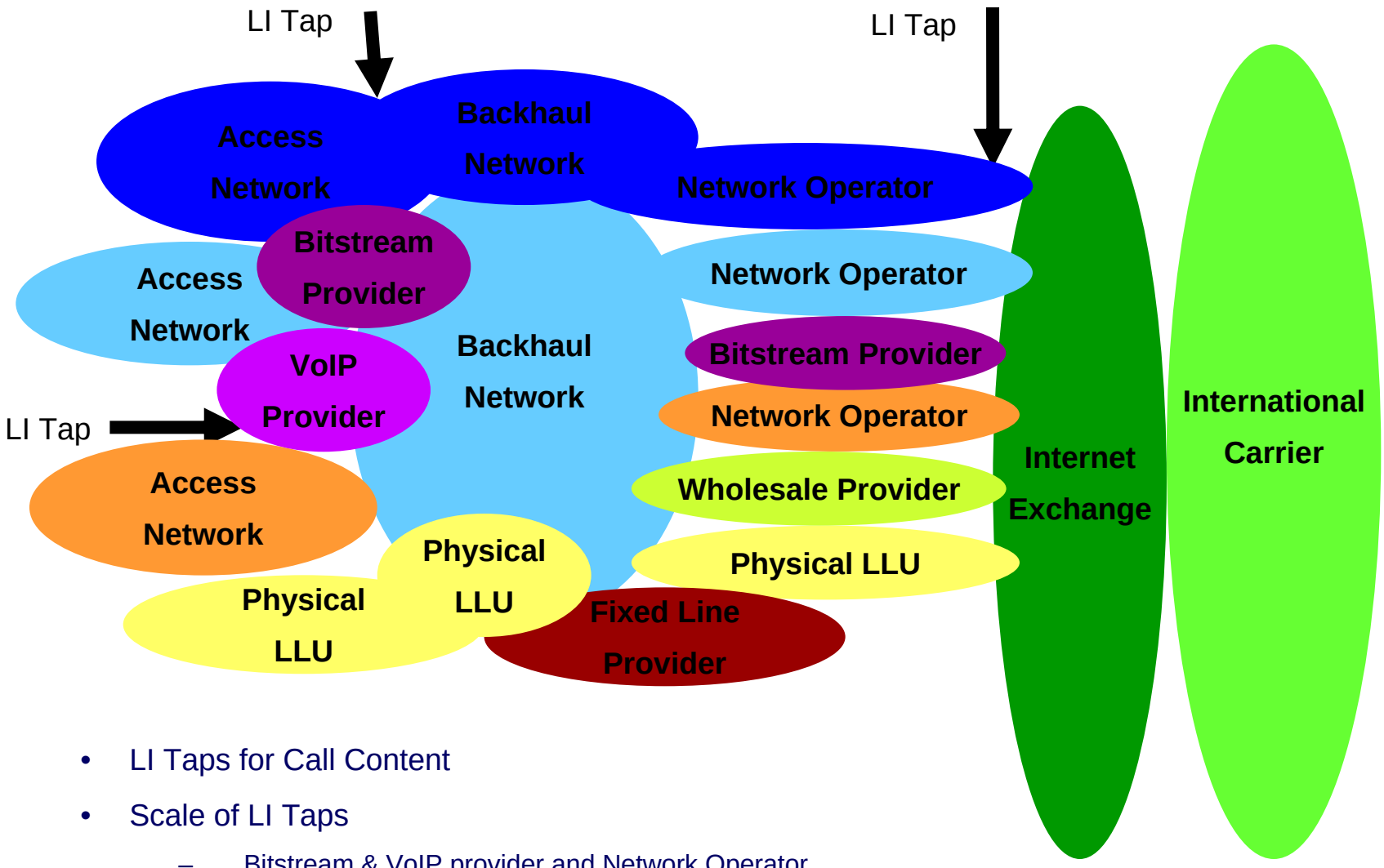


LI Tap with Incumbent in Telecoms Market



- Issues
  - All traffic force routed to international gateway – backbone costs
  - Performance intercepting all call data and content within volume
  - Mobile networks double NAT IP addresses obscuring them

LI Taps for Liberalised Telecoms Market



- LI Taps for Call Content
- Scale of LI Taps
  - Bitstream & VoIP provider and Network Operator
  - Minor Management and Operations

Public Safety for Liberalised Telecoms Market

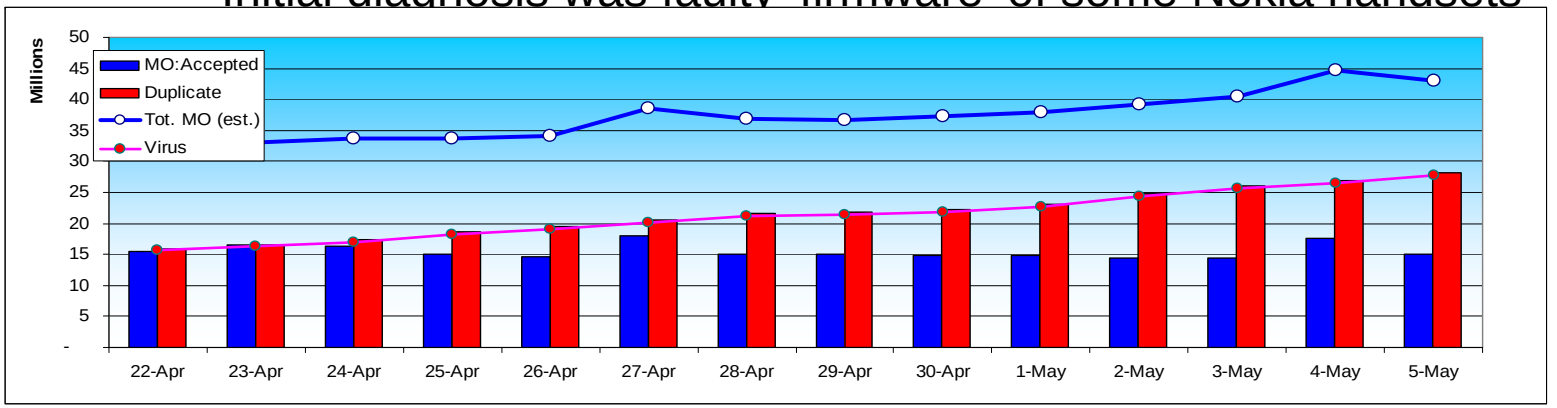
- Public Safety Partnership has challenges in developing capacity and capability plans in a telecoms liberalised market
  - Virus distribution among smart phones via MMS
  - Key loggers for collecting contacts from smart phones
  - SMS traffic overloading message switches and management
  - …

SMS Traffic

- Root cause analysis challenges
  - Customers complained of receiving duplicate SMS messages
  - Seeing huge volumes on SMSC

    > 33 Million duplicated SMSs daily

    Problem was growing by 4% a day
  - Initial diagnosis was faulty ‘firmware’ of some Nokia handsets



2 week period

33

Root Cause: Guardian Application

- Guardian client application causing havoc
  - Theft prevention software
  - Sends SMS when handset is turned on, and SIM or media changed

- Spreading like a virus
  - Seen in Middle East, Italy, Egypt, The Philippines
  - Accidentally being loaded on new phones by retailers, copies itself from media cards
  - More that 50,000 infected/ affected handsets
  - Currently limited to few specific DAs, but starting to see new ones
  - Sending up to 100 SMS messages a minute per handset to a non-existent number
    - » Application sending up to 10 a min, each fails And handset tries to send 10 times for each message

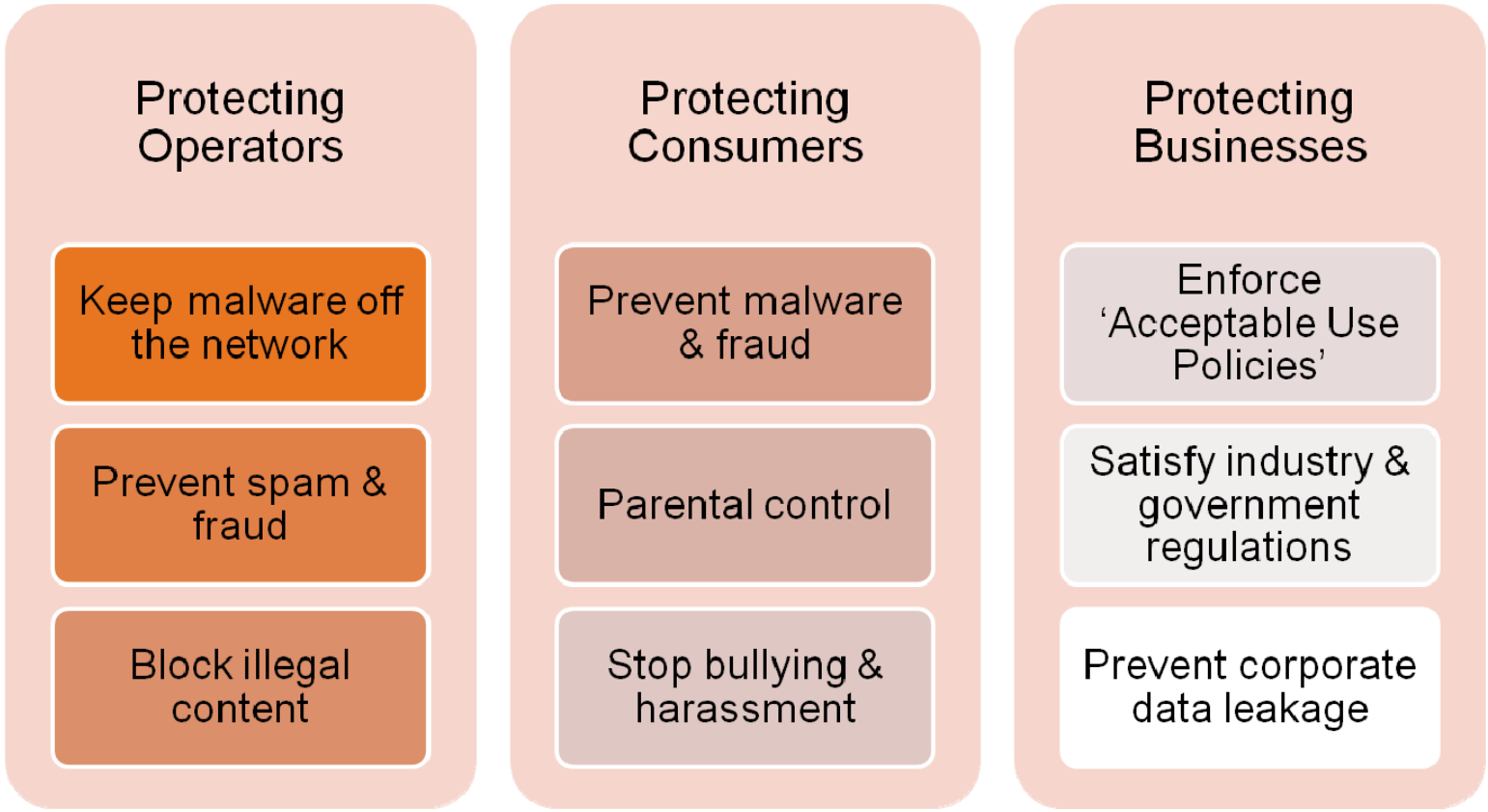
Still not out of the woods

- Temporary fix with SMSC changes to ACK the SMS
  - Dropped the number down to 300K per day
  - Rose back up to 2M SMS per day because of new Destination Addresses
- Very difficult to “clean”
  - Author provided an uninstall tool, but couldn’t easily deliver it to users (GPRS enablement, MMS capable handsets)
  - Hard to get marketing, operations, management to agree how to handle
    - » To Communicate cleansing
    - » Agree applications can be deleted from handset

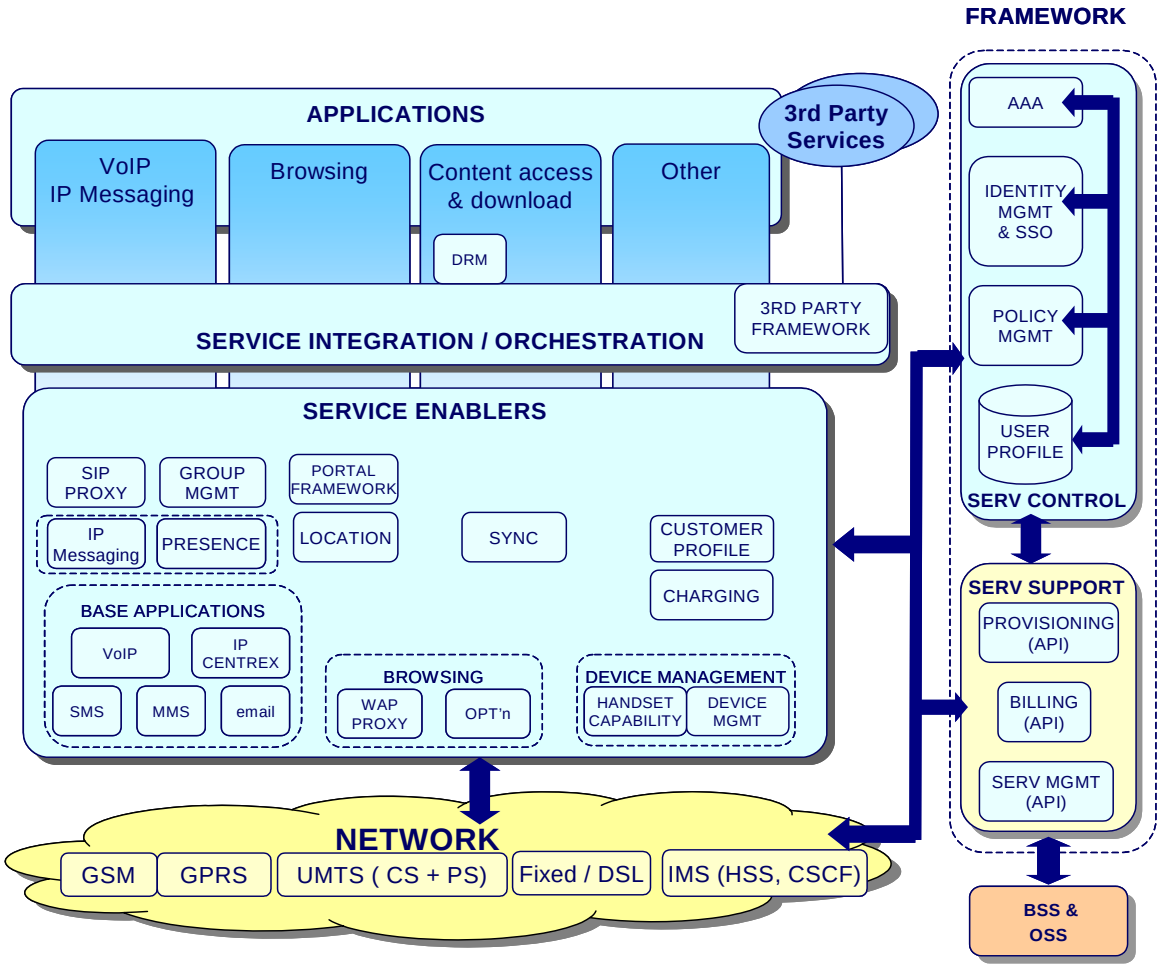
Audit and Enforcement

- For consumers the results of these development provide for an enhanced experience measured through the use of key performance indicators.
- Likewise the framework developed by the forum allows for all stakeholders to have metrics to measure against expected levels of behavior.
- Individuals who repeat bad levels of behavior after being warned can have penalties enforced against them.

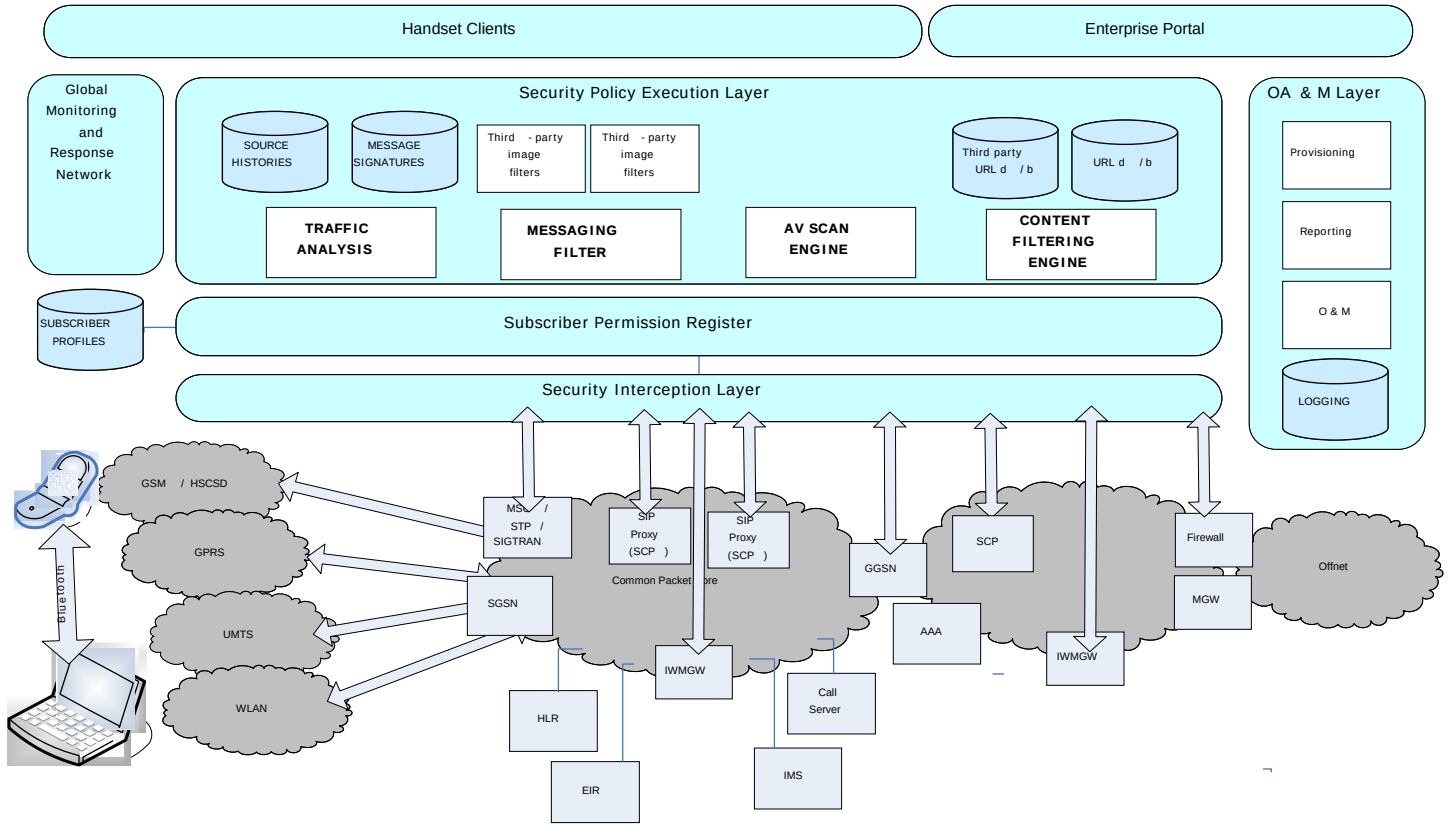
Security Control Framework



Telecom Services Architecture



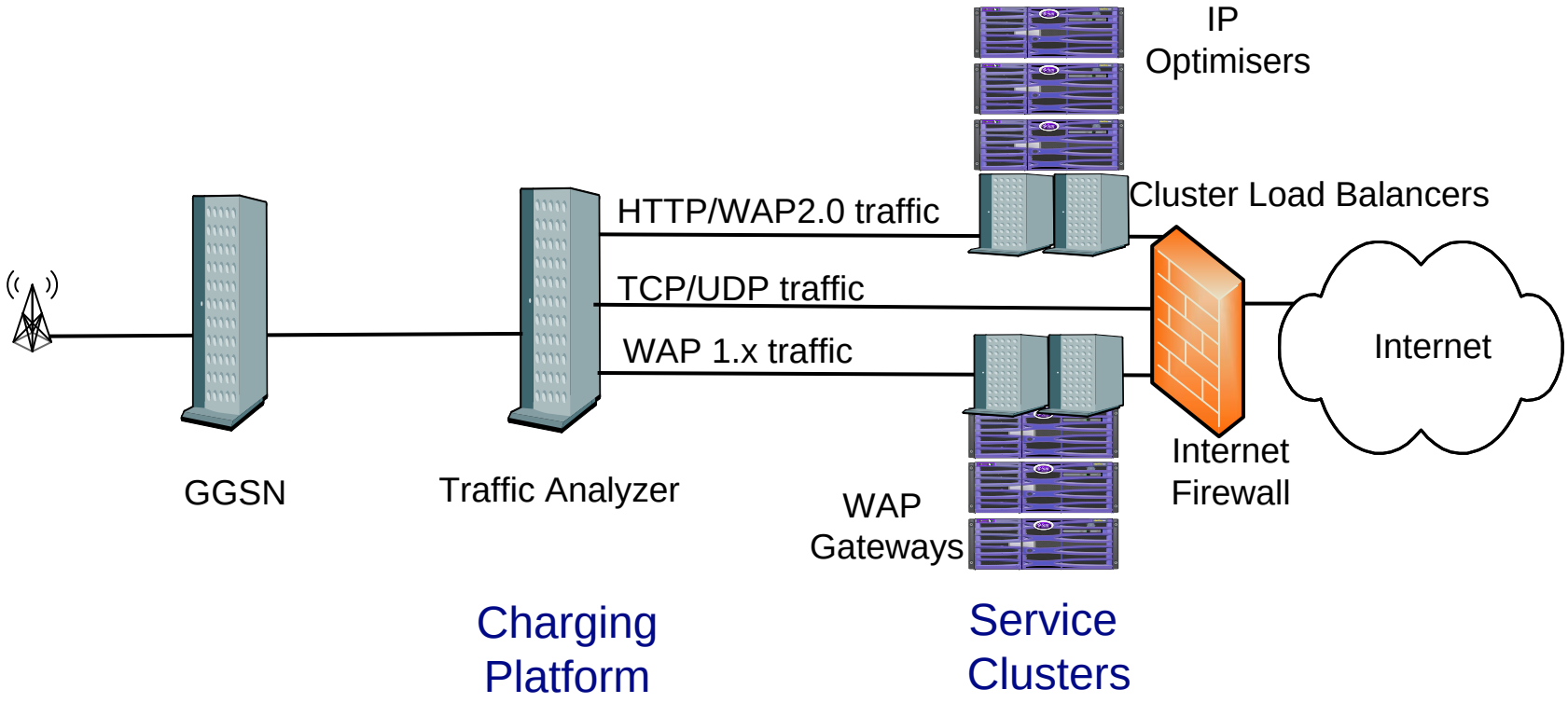
Hardware Architecture



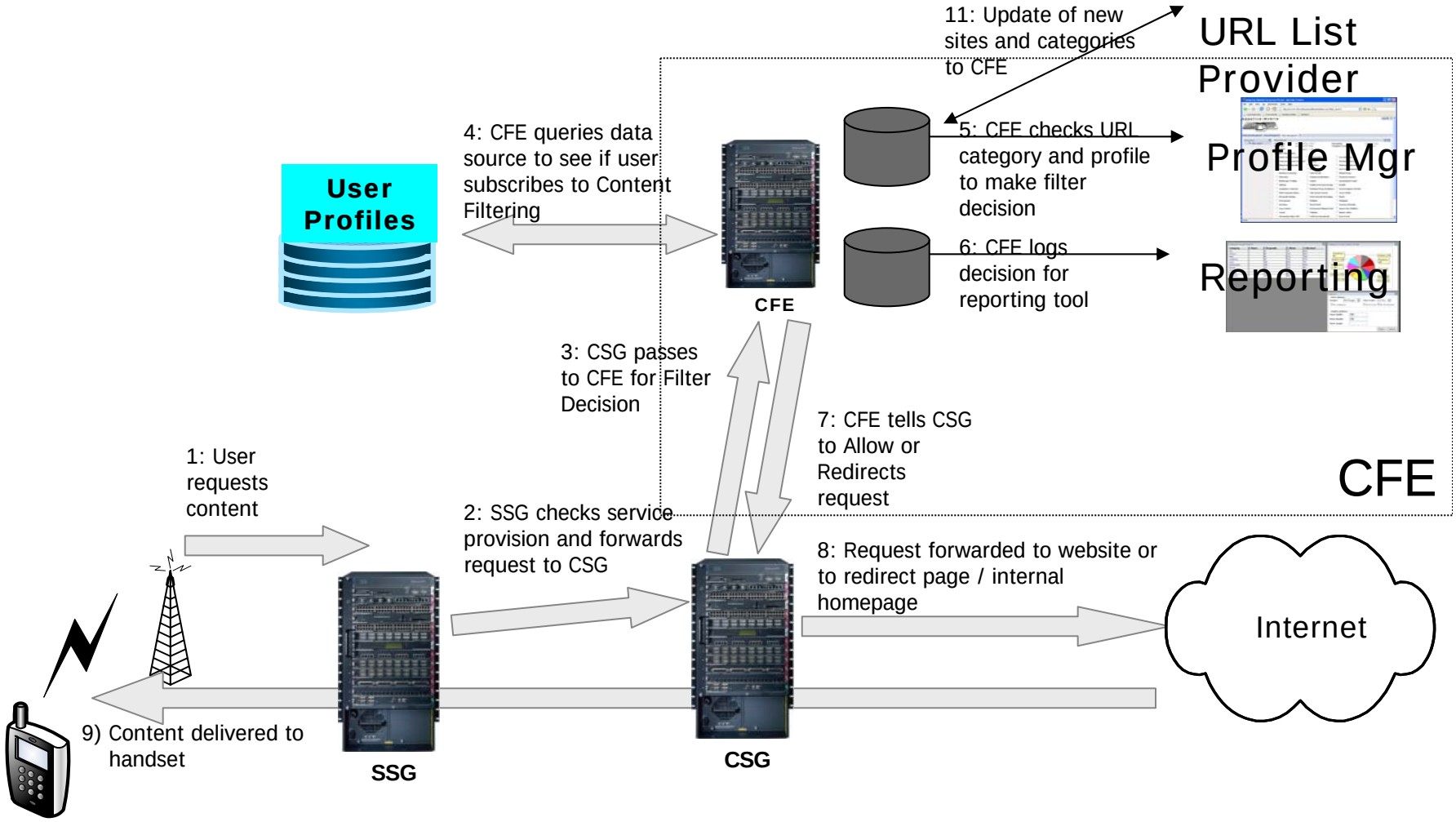
Traffic Control Technology

- Traffic management allowing monitoring and control of network traffic per application and per subscriber
  - Layer 7 deep packet inspection
  - Behavioural traffic analysis
  - Pattern matching of collaborative protocols
    - » P2P file sharing
    - » Instant Messaging
    - » Media Streaming
    - » Internet Telephony
  - Integrated QoS management
    - » Prioritization
    - » Shaping
    - » Blocking
  - Accounting
    - » Application aware
    - » Subscriber aware

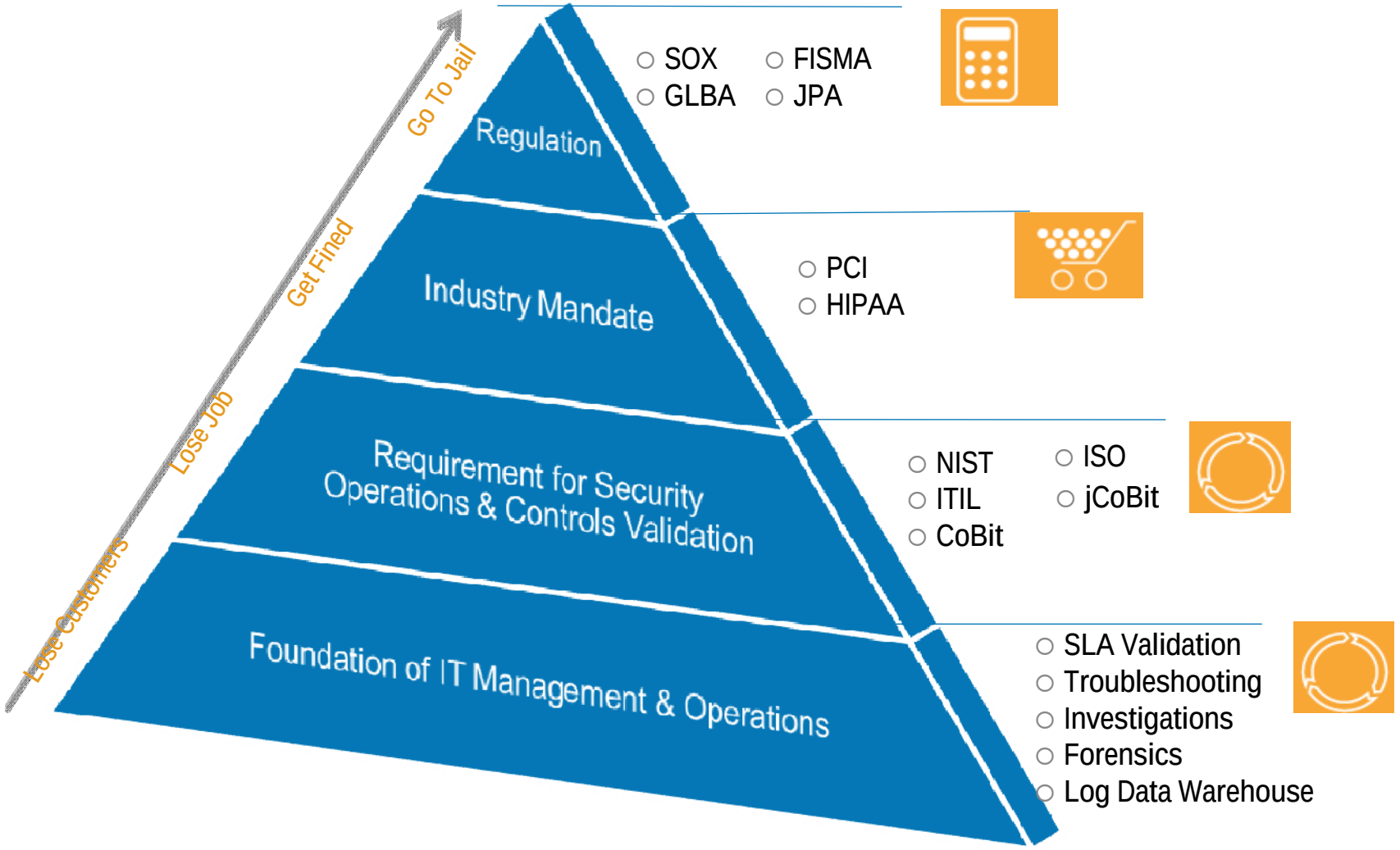
Network Architecture



Content Filtering System Logic Flow



Telecom Operator Governance



End