Presentation to European Defence Agency, Brussels

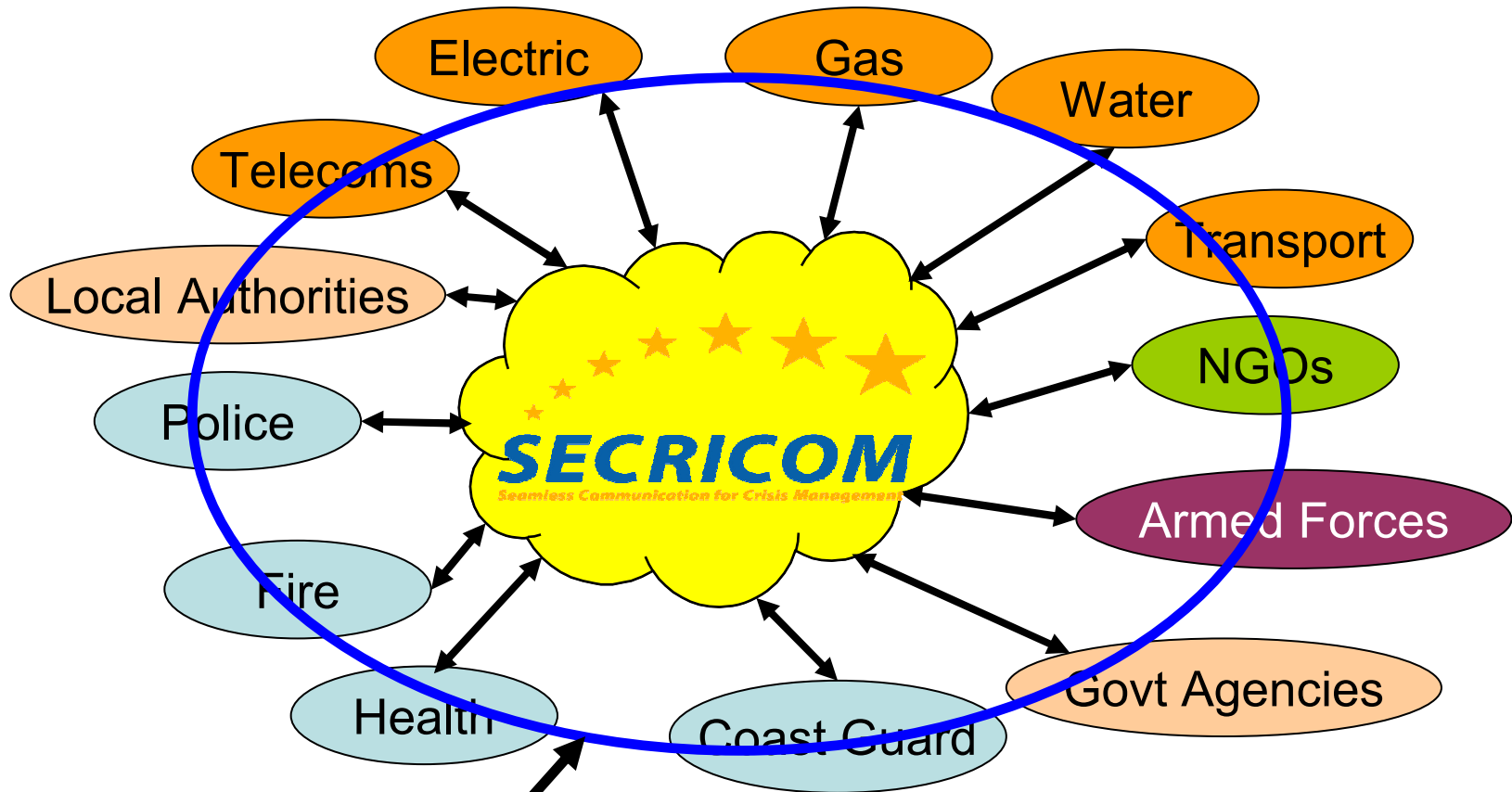Dr Ahmed Aldabbagh, Shaun O'Neill and John Stoodley

1/4/2009

Presentation objectives

- Outline Stakeholder requirements

- Introduce the project
  - Define SECRICOM
  - Vision
  - Programme & Partners

- Introduce the approach taken

- Give examples of architectures and technology

Introductory

Business Stakeholders

Electric · Gas · Water · Telecoms · Transport · Local Authorities · NGOs · Police · Armed Forces · Fire · Health · Coast Guard · Govt Agencies

SECRICOM
Seamless Communication for Crisis Management
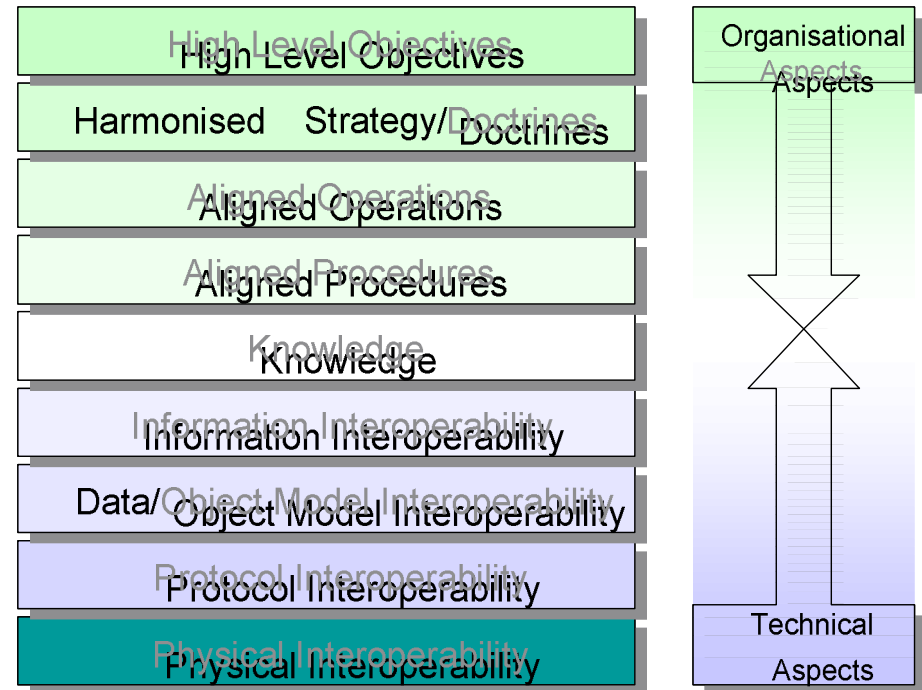
International Border

Interoperability

Definition:

The capability of two or more organisations or discrete parts of the same organisation to exchange decision-critical information and to use the information that has been exchanged.

Clearly, interoperability ranges from organisational to technical aspects all of which must be 'harmonised' in order to achieve full interoperability.
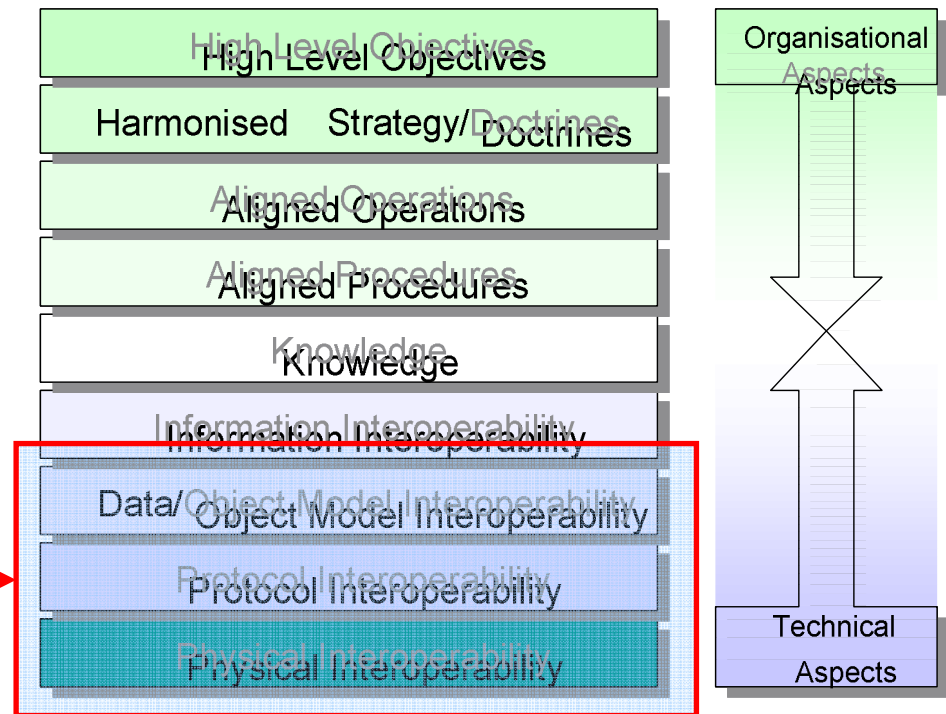
Layers of Interoperability

High Level Objectives

Harmonised Strategy/Doctrines

Aligned Operations

Aligned Procedures

Knowledge

Information Interoperability

Data/Object Model Interoperability

Protocol Interoperability

Physical Interoperability

Organisational Aspects

Technical Aspects

SECRICOM Project

Seamless Communication for Crisis Management

Scope: The technical aspects of Interoperability

Layers of Interoperability

High Level Objectives

Harmonised Strategy/Doctrines

Aligned Operations

Aligned Procedures

Knowledge

Information Interoperability

Data/Object Model Interoperability

Protocol Interoperability

Physical Interoperability

Organisational Aspects

Technical Aspects

Project Overview

- Dissemination (WP 11) — External interface
- Project management (WP 1) — Overall supervision
- Integration (WP 7) / Demonstrator creation (WP 10) — Building
- Communication Control Centre (WP 9)
- IPV6 Secure Communication (WP 6) — Enhancements
- Secure Wireless Communication (WP 3)
- Secure Agent Infrastructure (WP 4)
- Secure Docking Module (WP 5)
- Interoperable Recoverable And Extendable Network (WP 8) — Four technological pillars
- System Analysis and Design (WP 2) — Foundations

Consortium

Manufacturers & NGO

**Research & SMEs**

Universities

8

Vision

- Ability for responders to operate across different European emergency services/responder agencies as one cohesive unit at the time of crisis-level emergency

- Secure infrastructure for communication during a crisis with technical interoperability built into the design
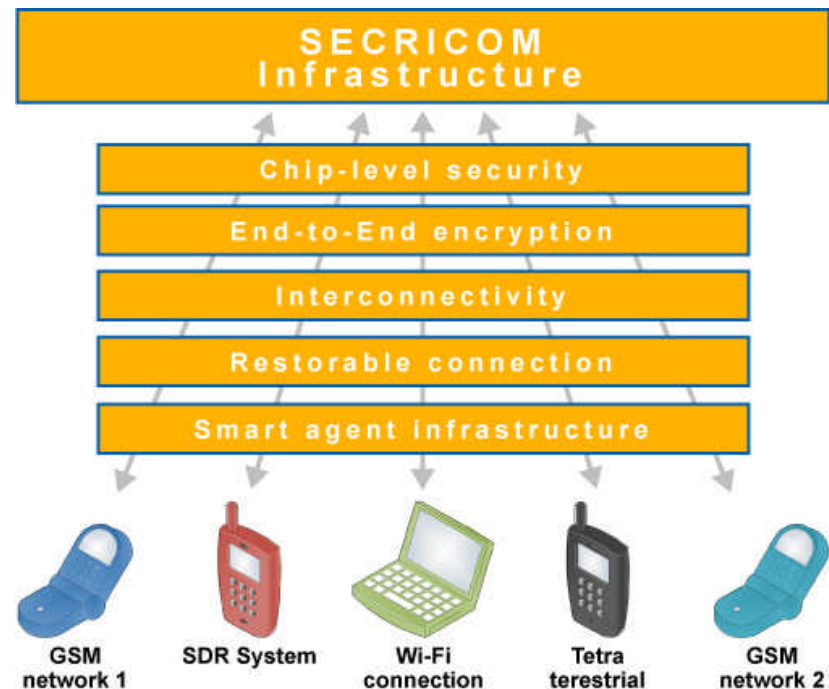
Aims

- Exploit the existing communication systems
- Enhance interoperability among heterogeneous secure communication systems
- Enhance interconnectivity between different networks and User Access Devices
- Interface towards emerging SDR systems
- Mitigate key capability gaps faced by users of existing systems

Approach
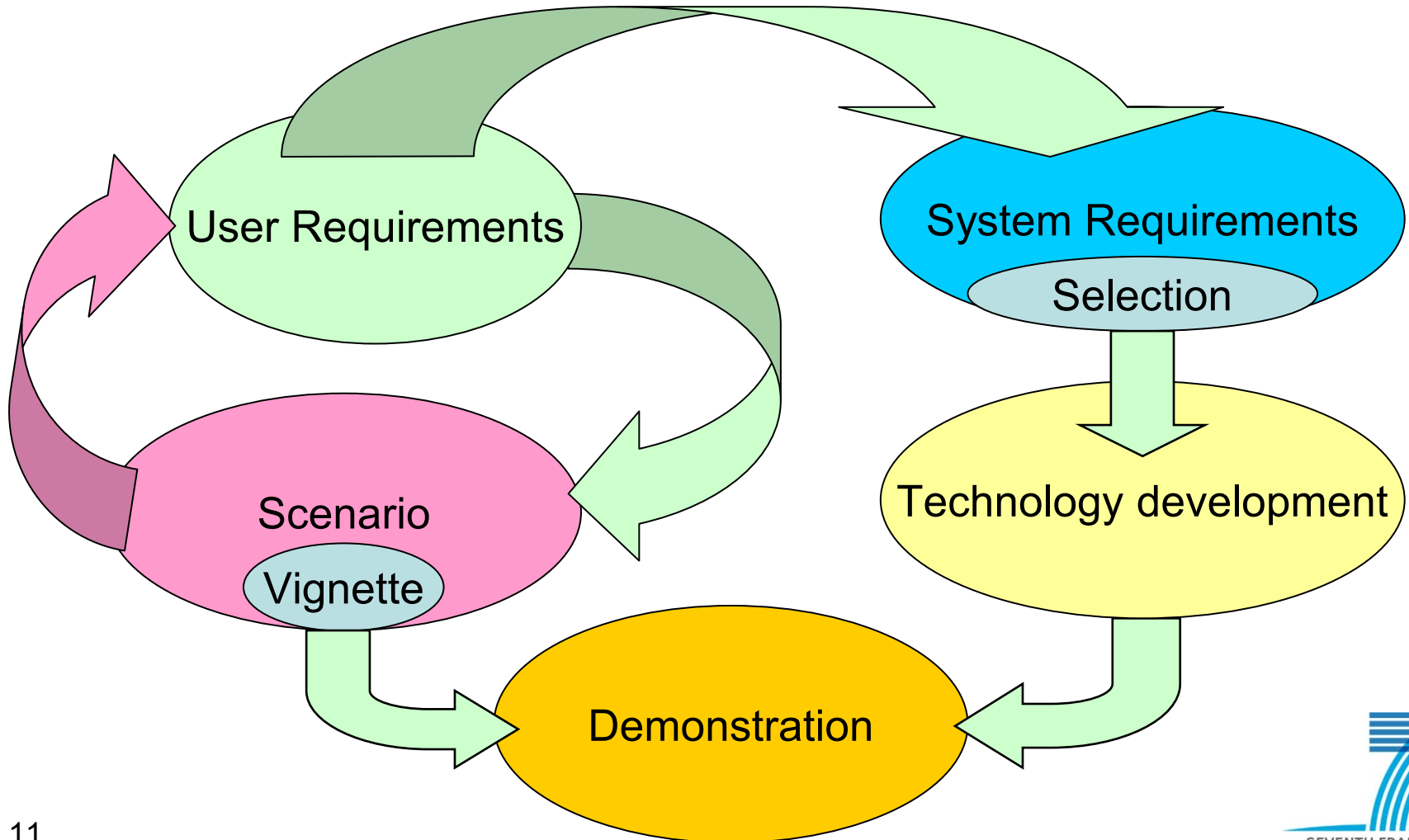
Related EU Projects

- **EULER**
European software defined radio for wireless in joint security operations

- **U-2010** - http://www.u-2010.eu/
FP6 funded project creating a vision of ubiquitous IP centric Government & Enterprise Next Generation Networks

- **PSC Europe** - http://www.publicsafetycommunication.eu/
Forum for Public Safety Communication Europe has been established in order to facilitate consensus building in the area of public safety communication and information management systems.

- **OASIS Project** - http://www.oasis-fp6.org/
The OASIS Project addresses the Strategic objective, "Improving Risk Management", of the second call for tender of the European Commission FP6 Information Society Technologies program.

- **CHORIST** - http://www.chorist.eu
FP6 funded project Integrating Communications for enHanced envirOnmental RISk management and citizens SafeTy-

- **OpenTC -** http://www.opentc.net/
The Open Trusted Computing (OpenTC) project targets traditional computer platforms as well as embedded systems such as mobile phones.
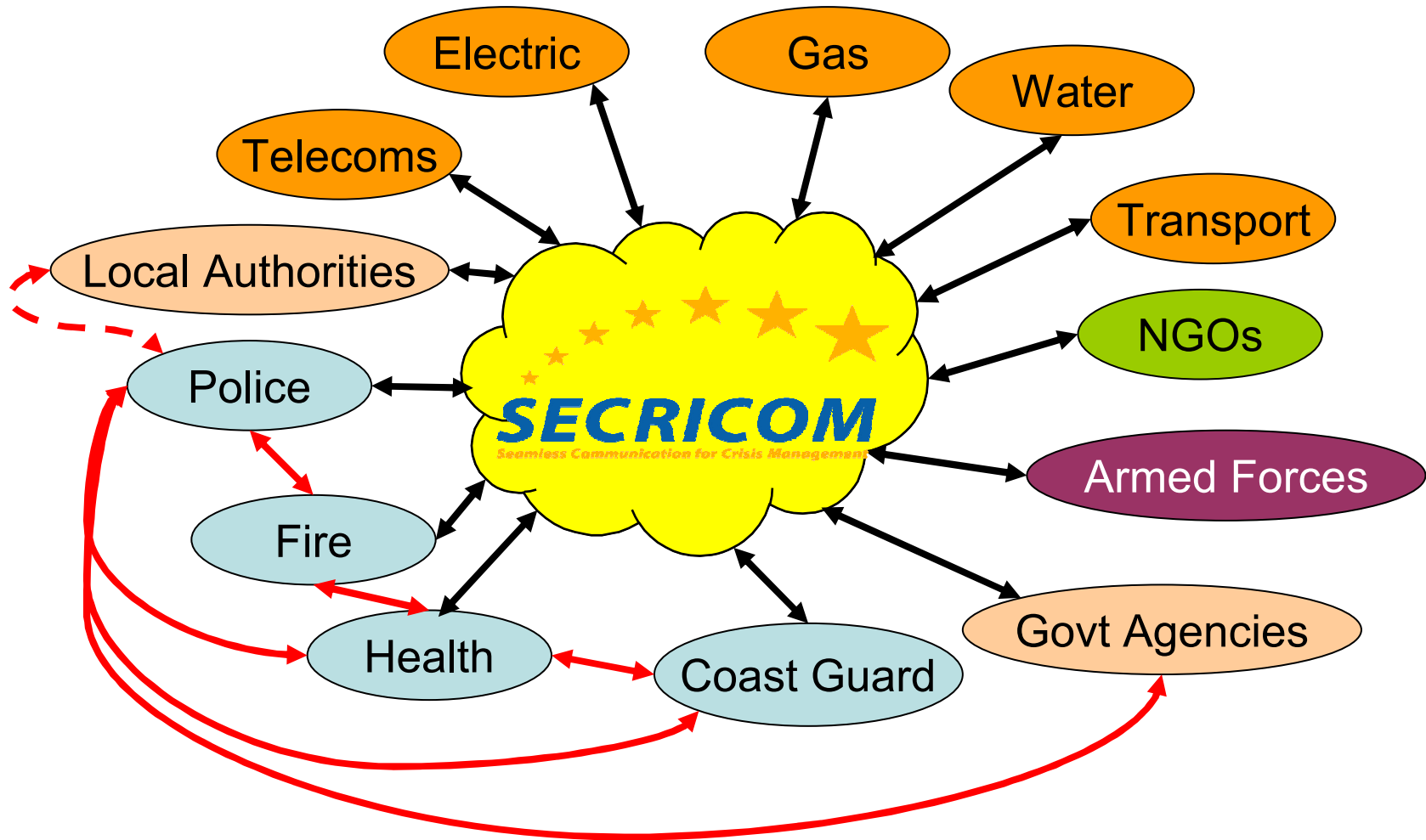
User Requirements

- Enable the user to clearly understand their objectives and/or command directives

- Expressed in terms of **what** the user wants to achieve

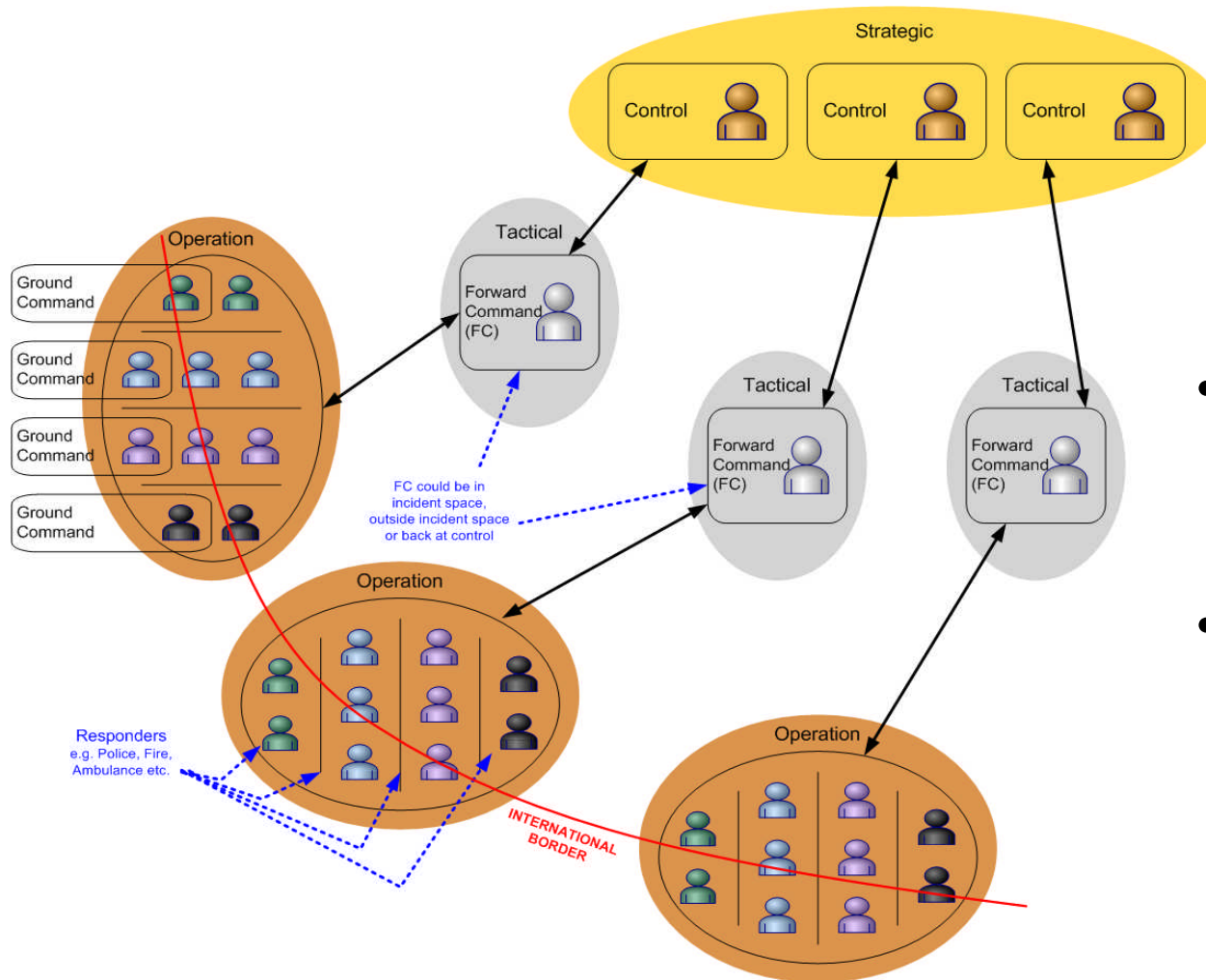- Discourages users from being seduced by technology

Principle of Crisis Management

Typical Information Exchange
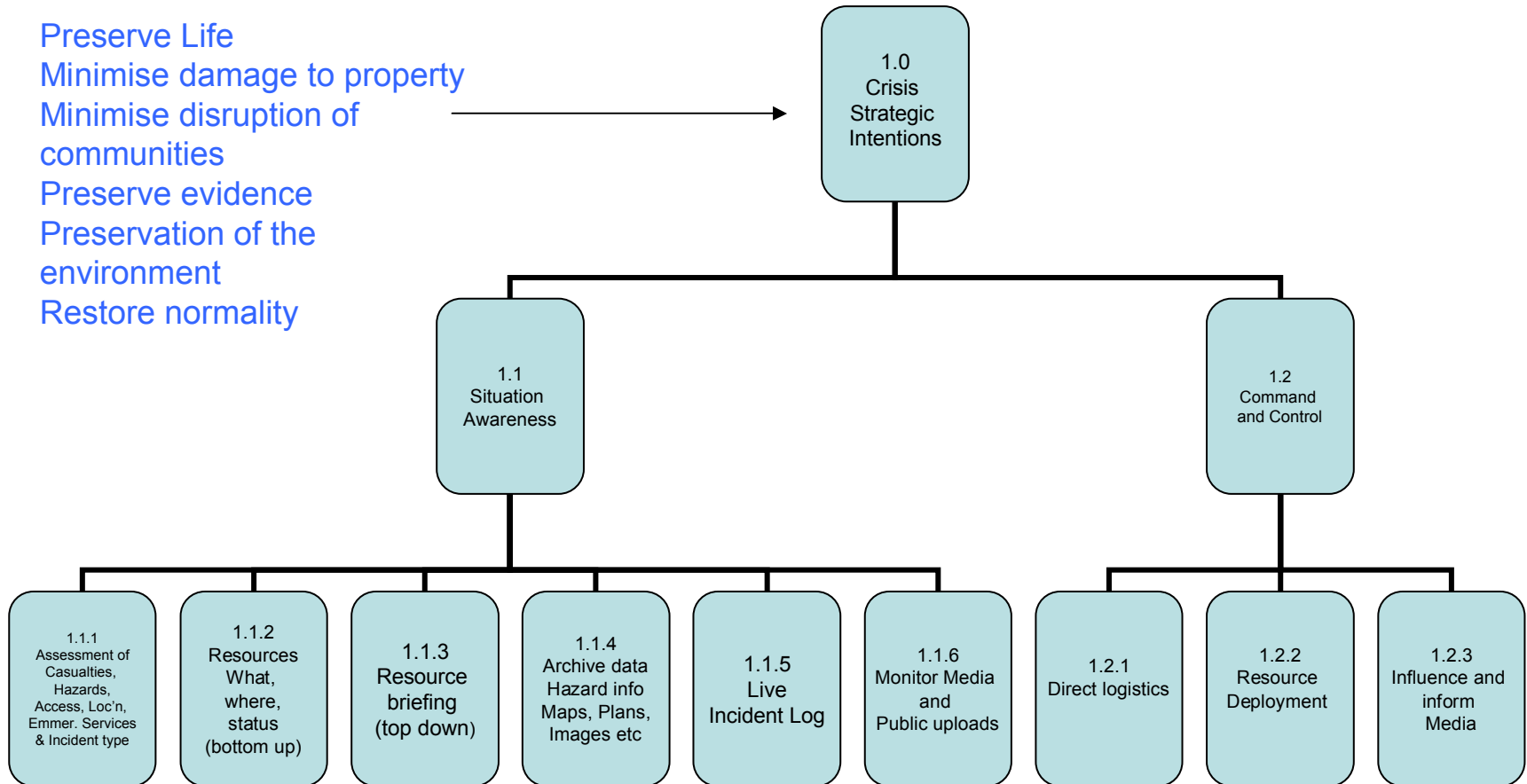
Typical C2 for the Emergency Services

- Extends across international borders
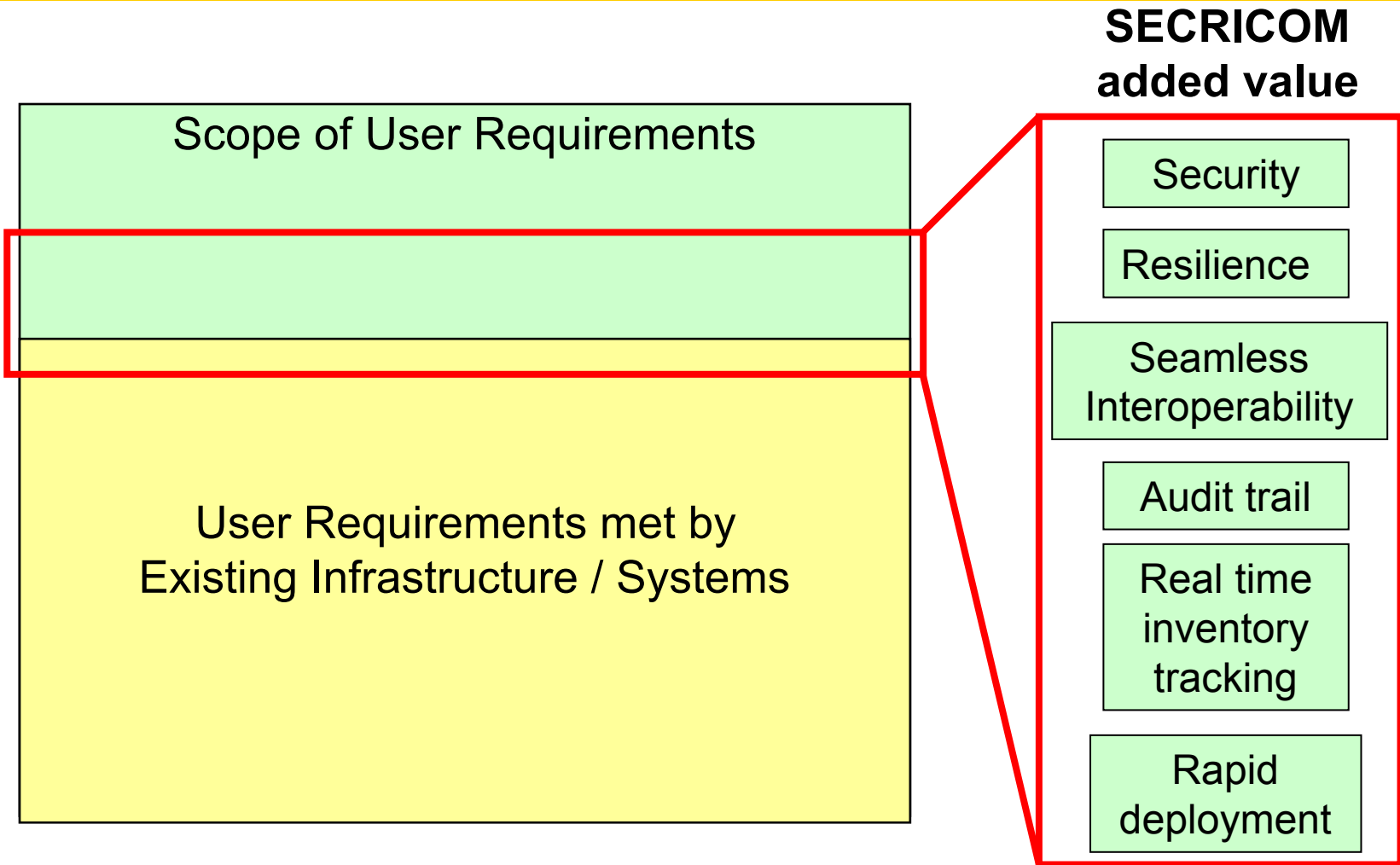- Extends across different agencies

High Level User Requirements

Preserve Life
Minimise damage to property
Minimise disruption of communities
Preserve evidence
Preservation of the environment
Restore normality

1.0 Crisis Strategic Intentions

1.1 Situation Awareness

1.2 Command and Control

1.1.1 Assessment of Casualties, Hazards, Access, Loc'n, Emmer. Services & Incident type

1.1.2 Resources What, where, status (bottom up)

1.1.3 Resource briefing (top down)

1.1.4 Archive data Hazard info Maps, Plans, Images etc

1.1.5 Live Incident Log

1.1.6 Monitor Media and Public uploads

1.2.1 Direct logistics

1.2.2 Resource Deployment

1.2.3 Influence and inform Media

Capability Gaps - illustrative

SECRICOM added value

Scope of User Requirements
User Requirements met by Existing Infrastructure / Systems

- Security
- Resilience
- Seamless Interoperability
- Audit trail
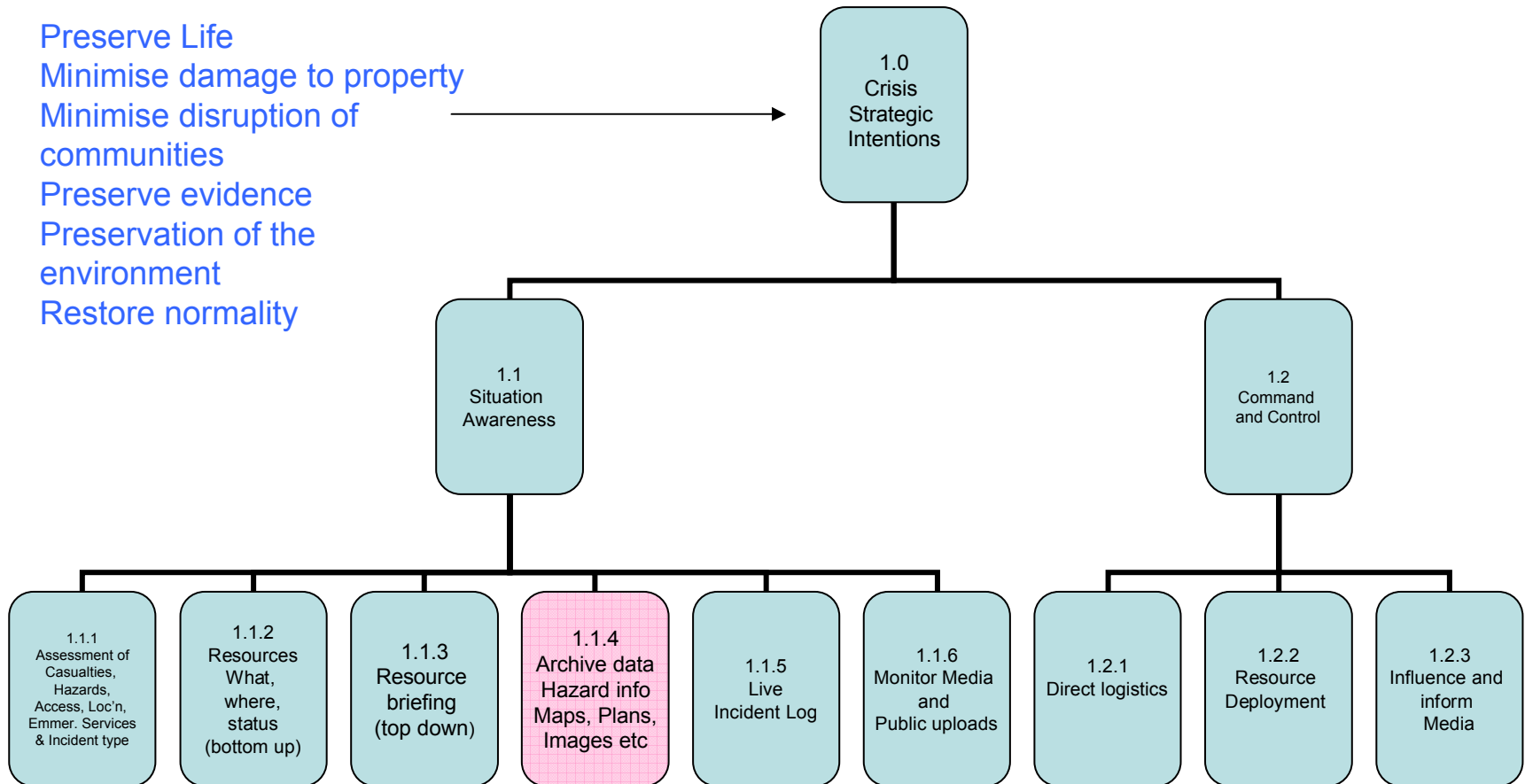- Real time inventory tracking
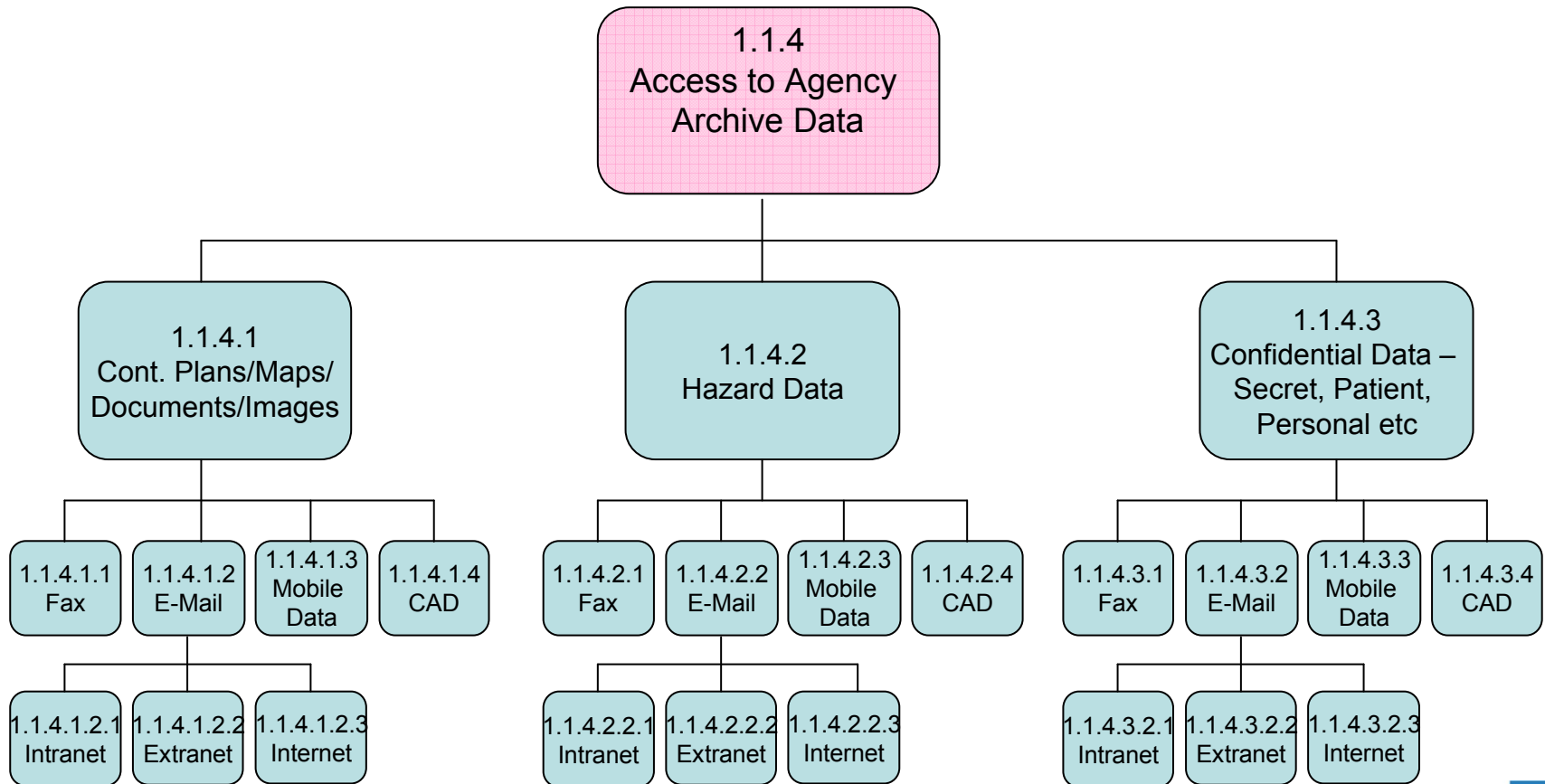- Rapid deployment

System Requirements

- Derived from the user requirements

- Concerned with the minimum required functionality necessary to meet the user requirement

- Expressed in an appropriate fashion, e.g. tree and/or architecture diagrams

- Must take existing systems into account
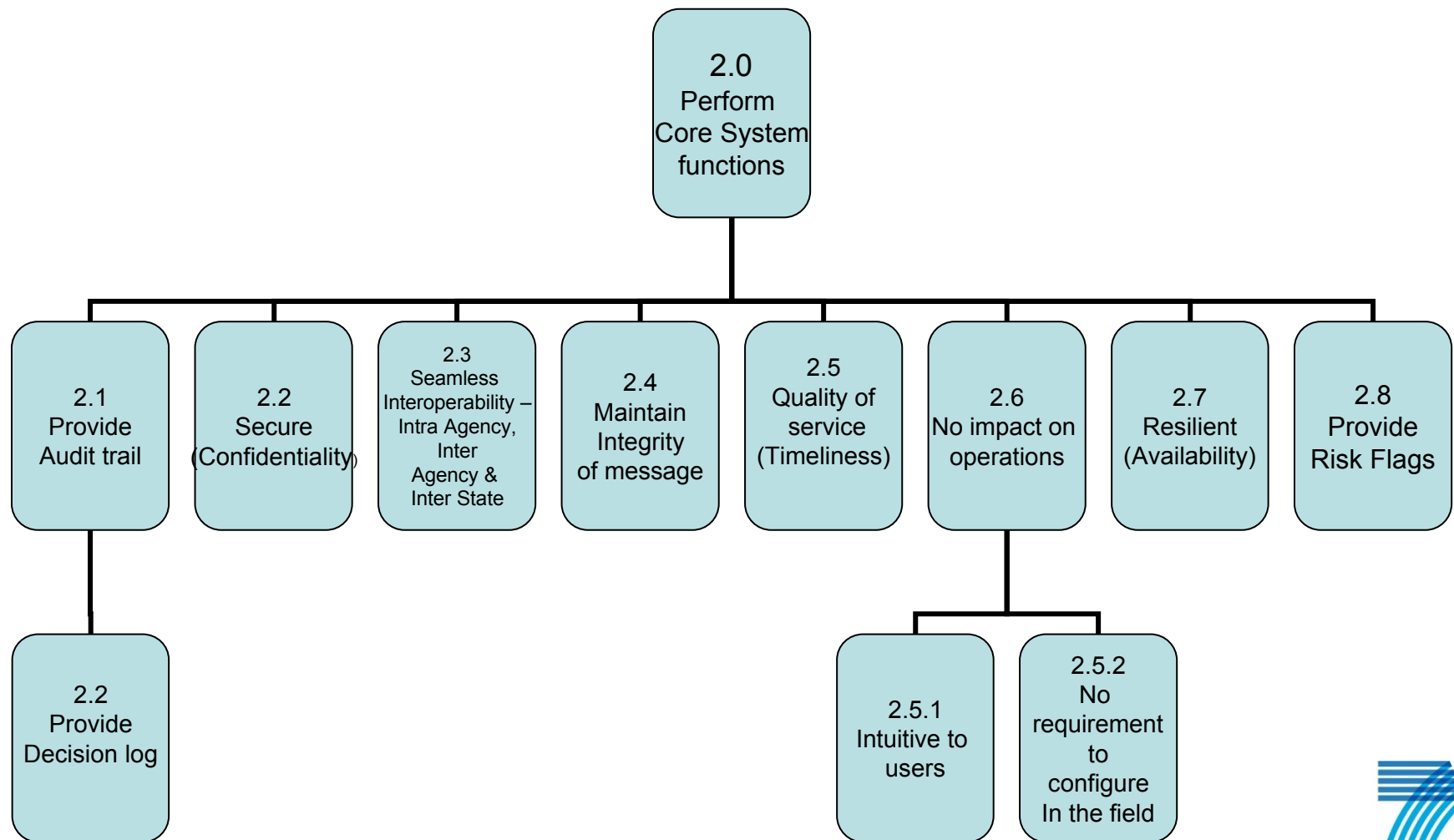
Example of Procedure

Preserve Life
Minimise damage to property
Minimise disruption of communities
Preserve evidence
Preservation of the environment
Restore normality

→

1.0 Crisis Strategic Intentions

1.1 Situation Awareness

1.2 Command and Control

1.1.1 Assessment of Casualties, Hazards, Access, Loc'n, Emmer. Services & Incident type

1.1.2 Resources What, where, status (bottom up)

1.1.3 Resource briefing (top down)

1.1.4 Archive data Hazard info Maps, Plans, Images etc

1.1.5 Live Incident Log

1.1.6 Monitor Media and Public uploads

1.2.1 Direct logistics

1.2.2 Resource Deployment

1.2.3 Influence and inform Media

Derivation of System Requirements

Core System Functions

System Architecture and Solution Technologies

Clear <u>Need</u> for Communications that can be relied upon, that is both *Ubiquitous and Interoperable*

Communications System Architecture

- <u>Ubiquitous</u> communications requires usage of as many communications, and avoidance of reliance on a single system

  - Make simultaneous use of 3G, GSM, WiFi, WiMax, Satellite, SDR, etc

  - Aim for seamless switch over with minimal impact to user/business

- <u>Interoperable</u> communications requires usage of open/non-proprietary standards for system, hardware and software

  - Network: IPv6 as the principle standard for networking: future-proof

  - Wireless: 3G, GSM, WiFi, WiMax, TETRA, Satellite, etc
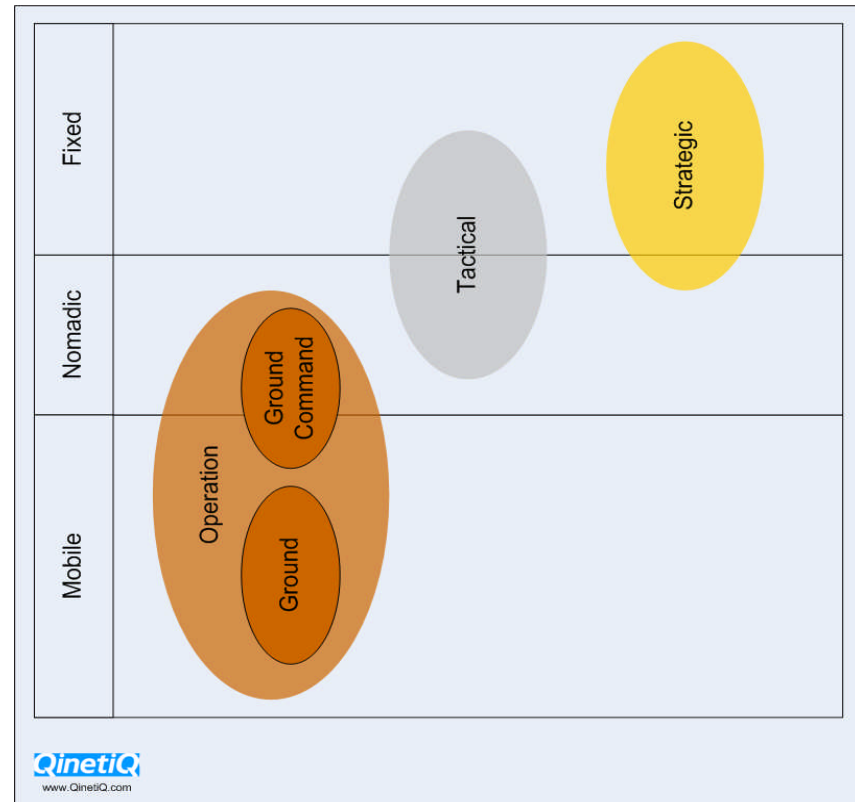
  - Fixed: Ethernet

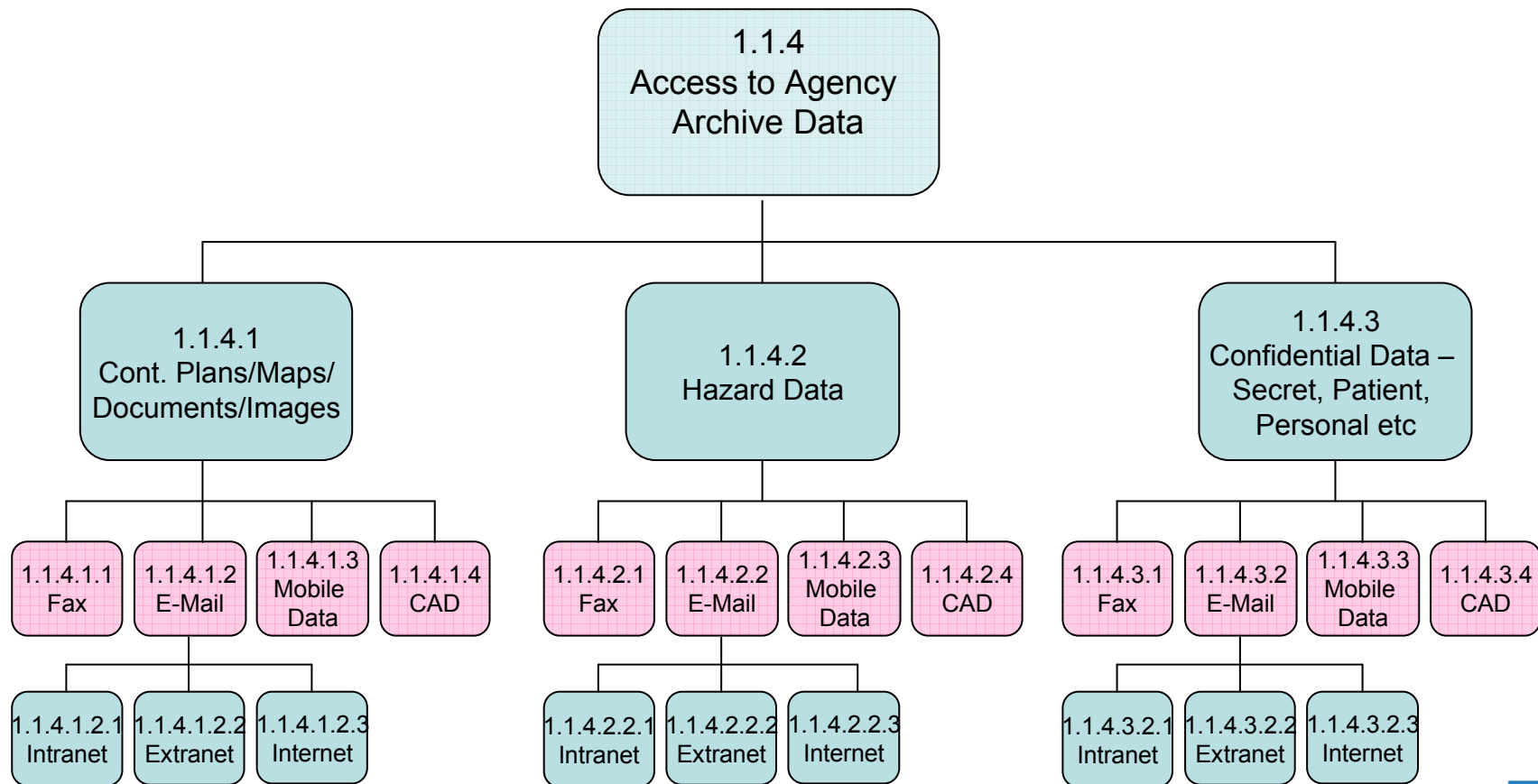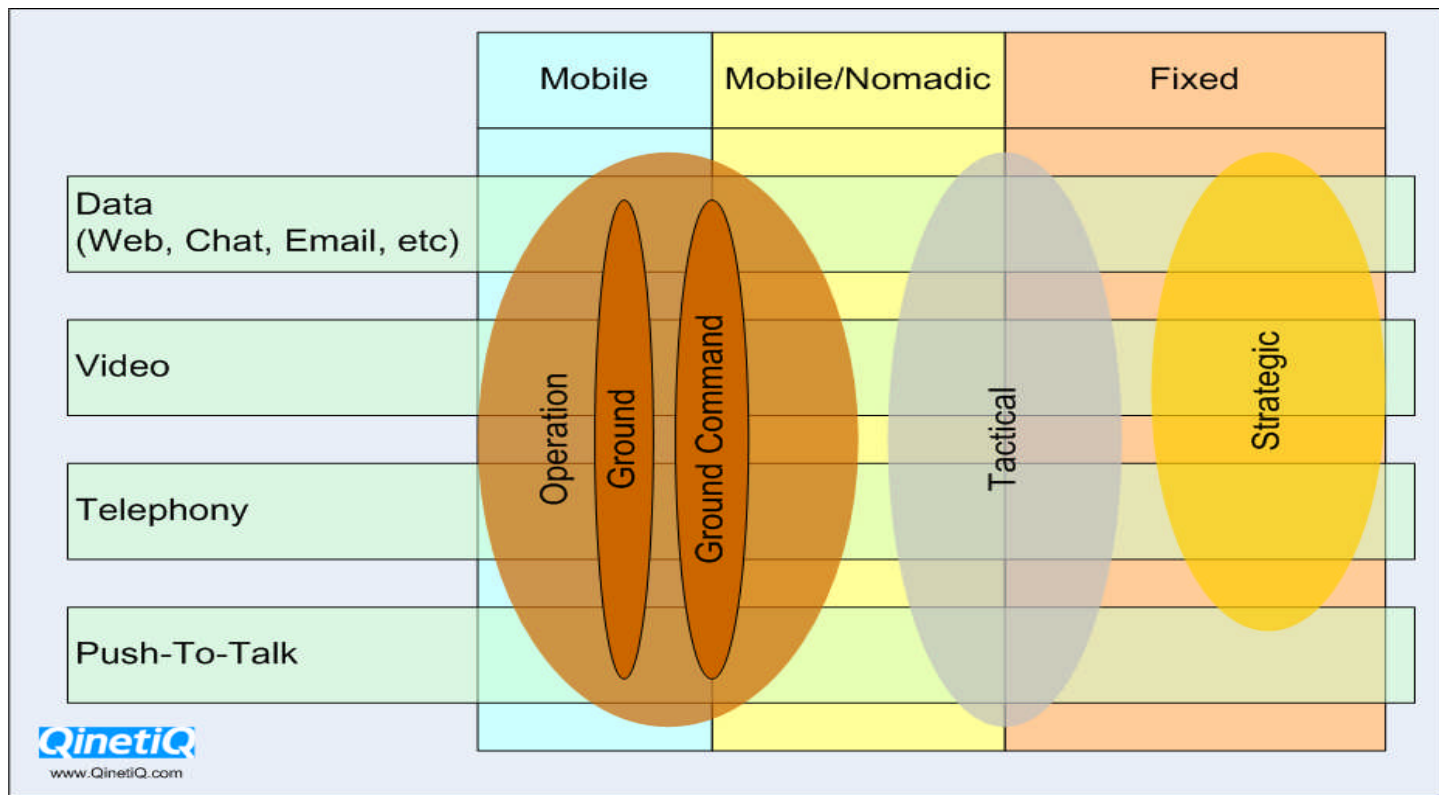# Communications System Features for SECRICOM
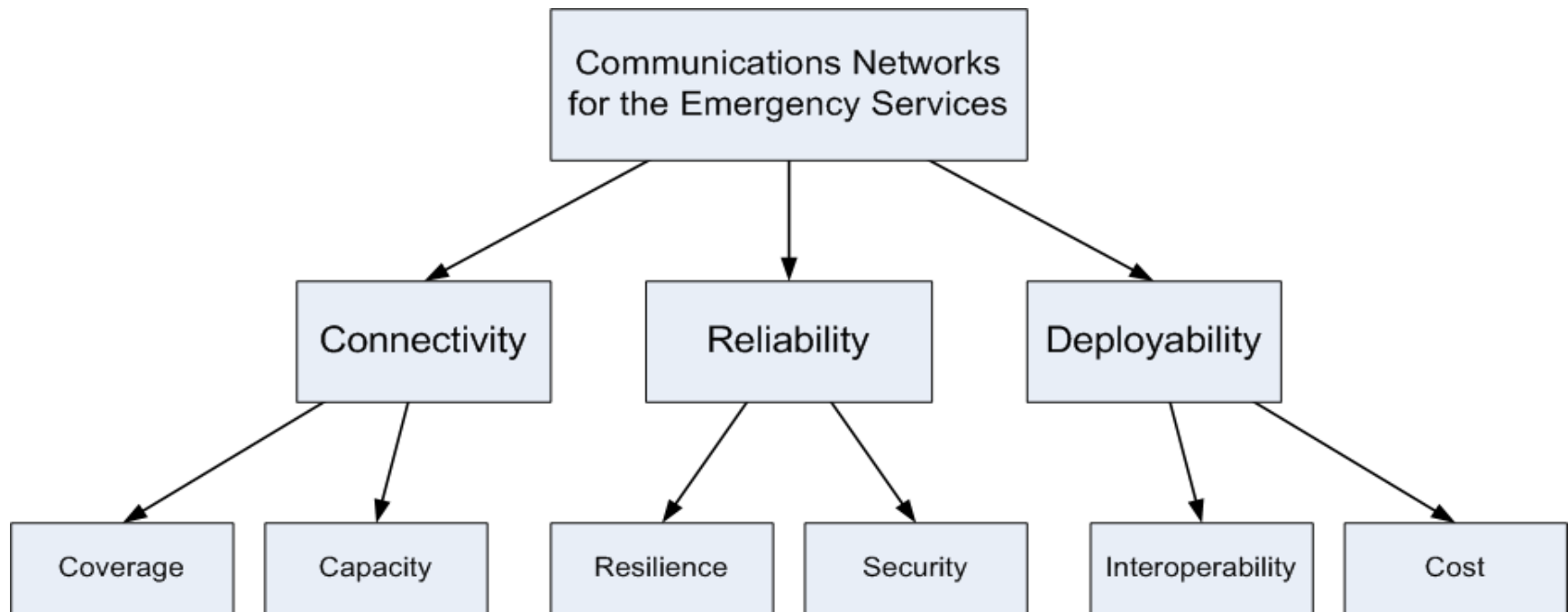
Type of Users

- <u>Fixed</u>, e.g. office

- <u>Nomadic</u>, e.g. deployable office

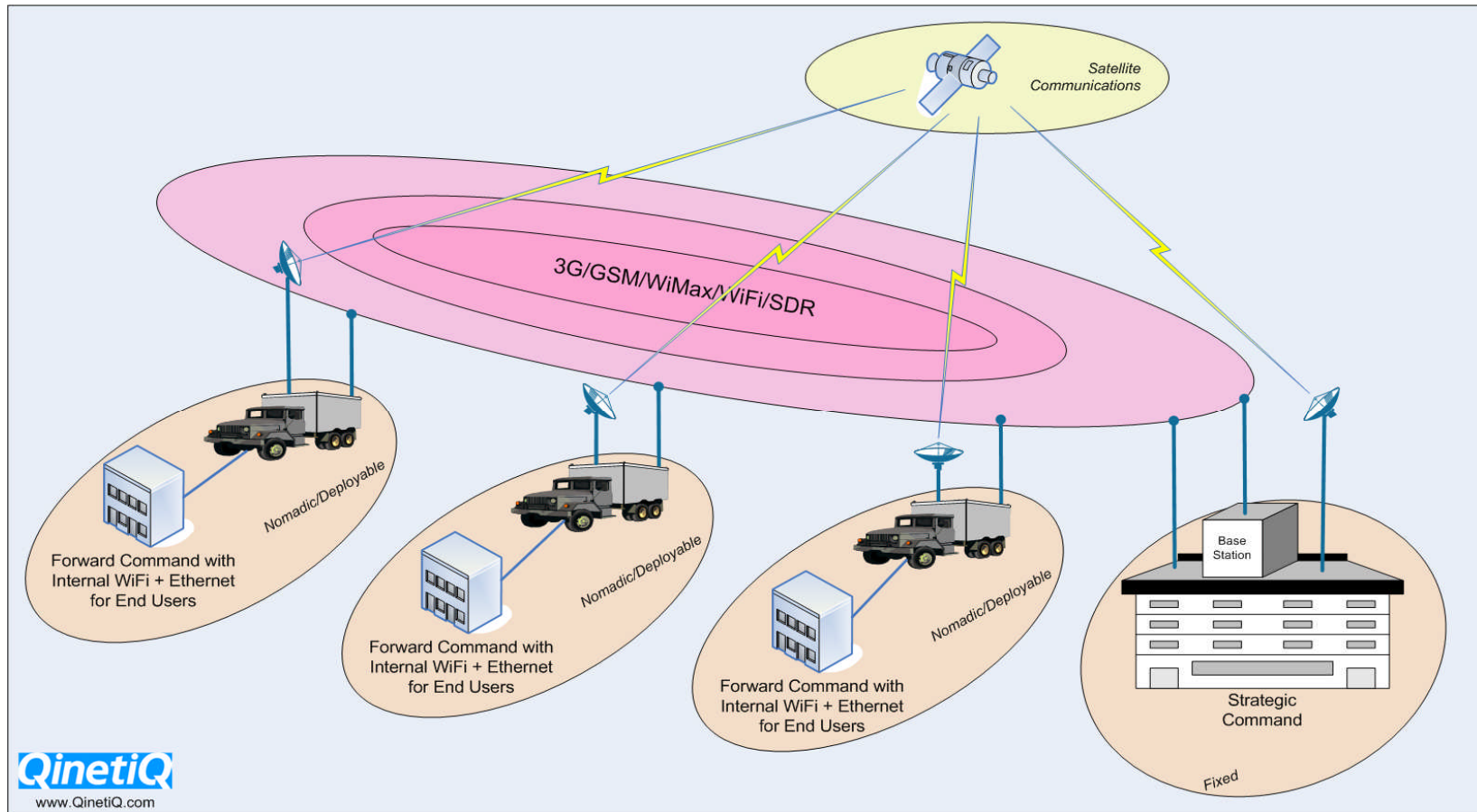- <u>Mobile</u>, e.g. land/air/water transport or on-foot

Type of Traffic

SECRICOM
Seamless Communication for Crisis Management

```
                        1.1.4
                   Access to Agency
                     Archive Data

        1.1.4.1              1.1.4.2              1.1.4.3
     Cont. Plans/Maps/      Hazard Data      Confidential Data –
    Documents/Images                          Secret, Patient,
                                                Personal etc

  1.1.4.1.1  1.1.4.1.2  1.1.4.1.3  1.1.4.1.4    1.1.4.2.1  1.1.4.2.2  1.1.4.2.3  1.1.4.2.4    1.1.4.3.1  1.1.4.3.2  1.1.4.3.3  1.1.4.3.4
    Fax       E-Mail    Mobile      CAD           Fax       E-Mail    Mobile      CAD           Fax       E-Mail    Mobile      CAD
                         Data                                          Data                                          Data

        1.1.4.1.2.1  1.1.4.1.2.2  1.1.4.1.2.3   1.1.4.2.2.1  1.1.4.2.2.2  1.1.4.2.2.3   1.1.4.3.2.1  1.1.4.3.2.2  1.1.4.3.2.3
         Intranet     Extranet     Internet      Intranet     Extranet     Internet      Intranet     Extranet     Internet
```
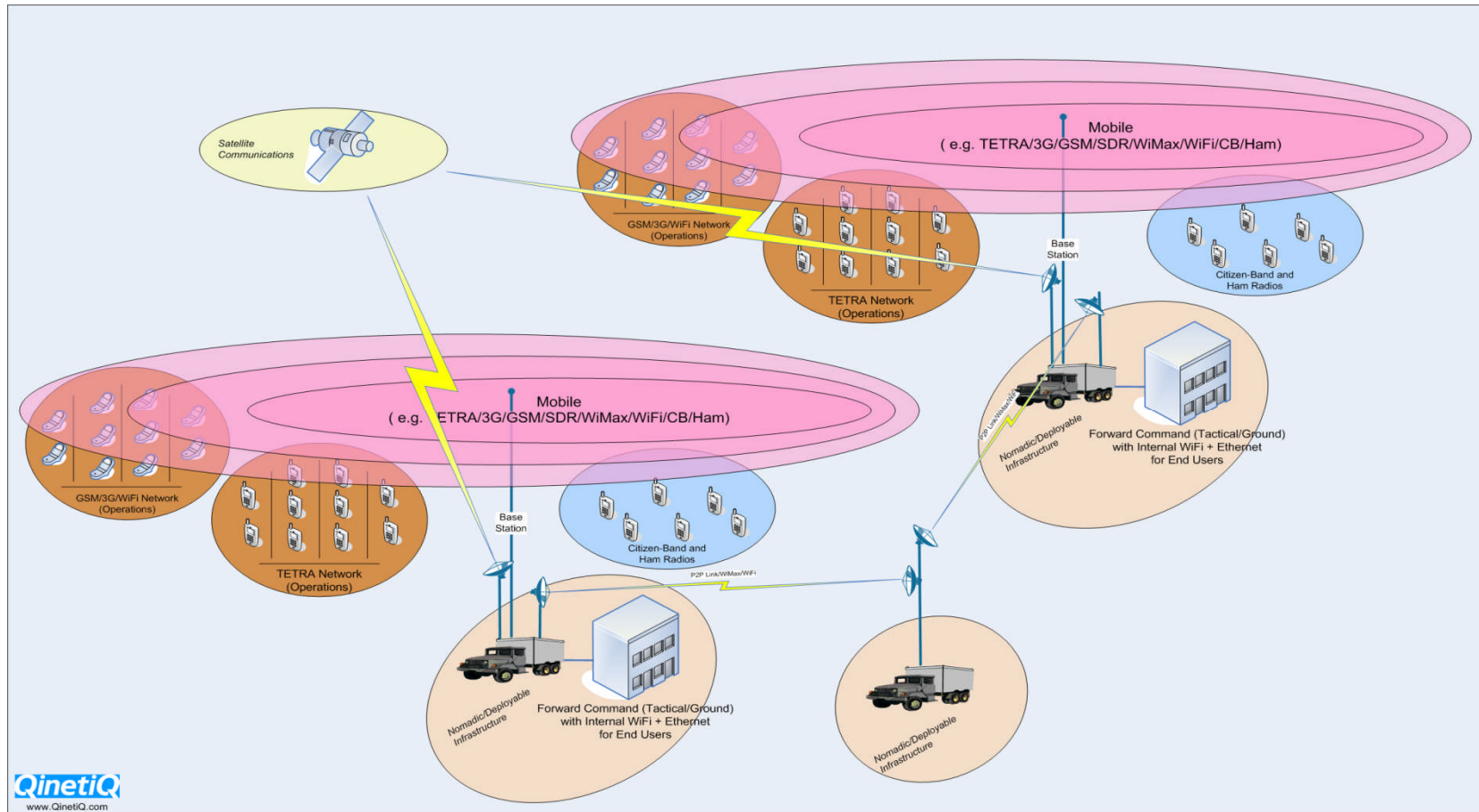
SEVENTH FRAMEWORK PROGRAMME

Type of Traffic for Users
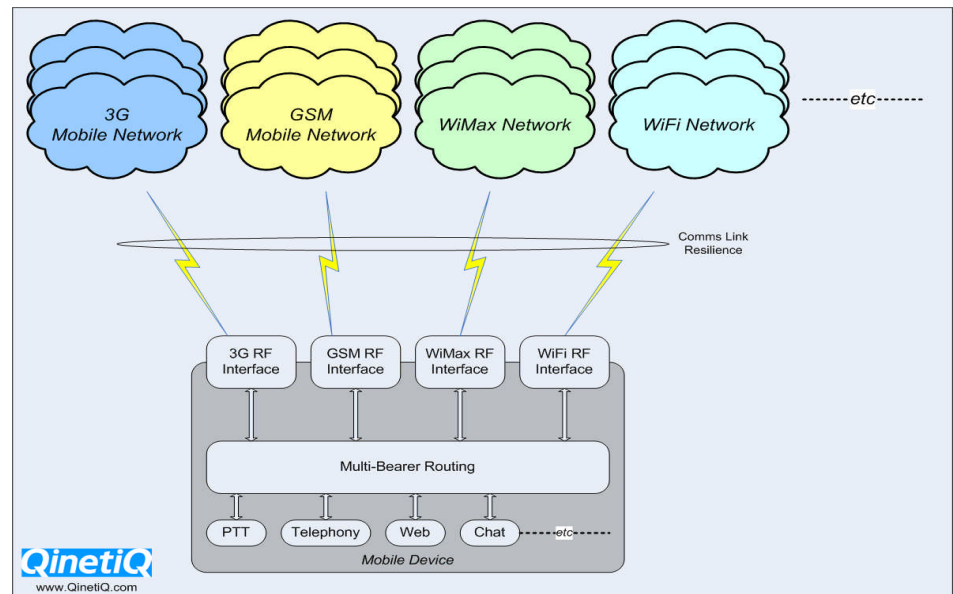
Strategic/Forward Command Communications

Forward-Command/Operations Communications

Delivering Resilience

Resilience can be best carried forward to the frontline and into the operations space by the use of mobile communication devices which are

- – Open
- – Capable of communicating using multiple standards

Holistic High Level View

The communications system architecture allows:

– Technical interoperability, thus able to extend communications across different agencies and across different countries

– Technical expandability, thus able to extend communications to places where communications not usually available achieving ubiquitous operations
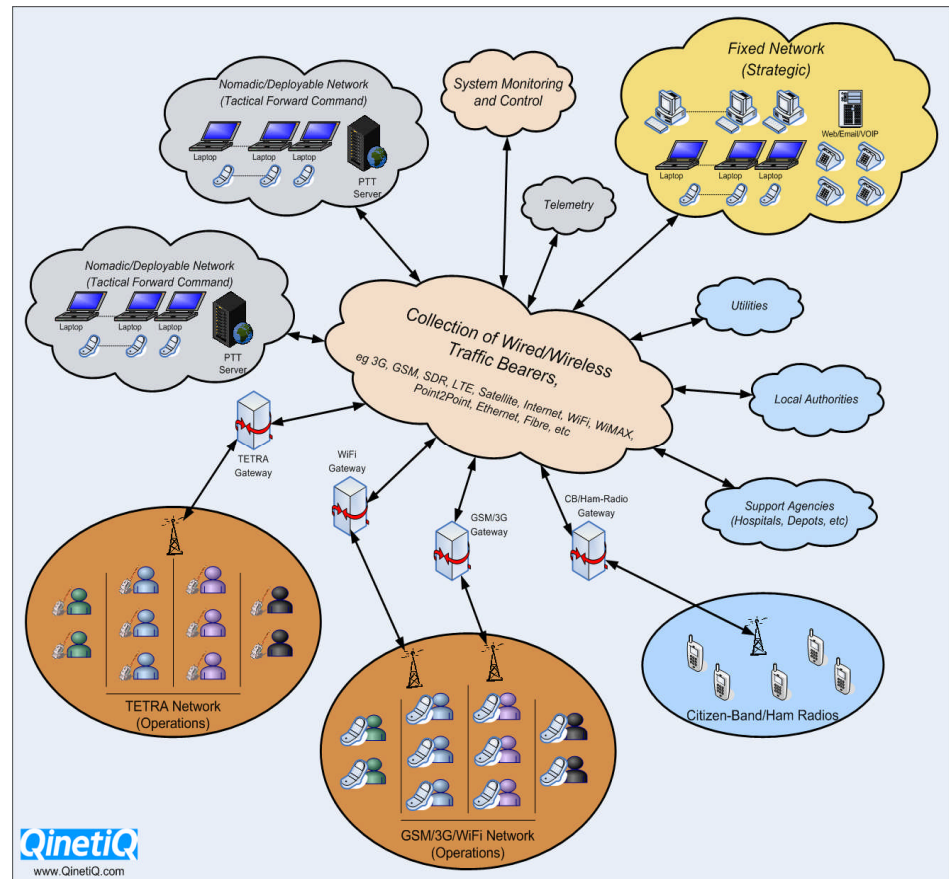
Operator High Level View
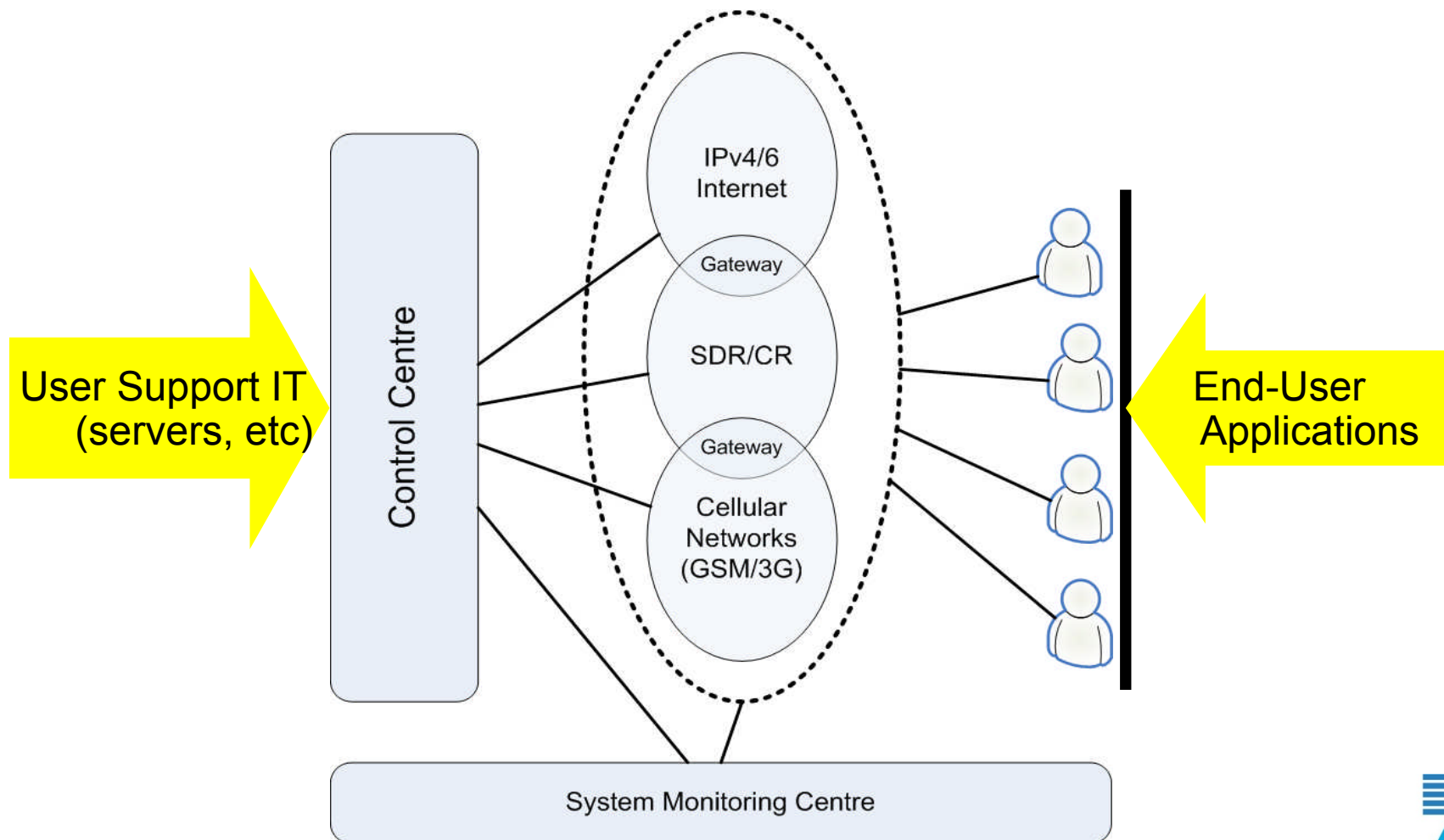
Application Level Resilience

Push-to-talk load distribution

- Client devices
  - Login – using DNS Server

- DNS Servers
  - Select switch with lowest load or first available switch

- Switch
  - Select first available SIP Server

- SIP Server
  - Create session on RTP Server with lowest load balance

- RTP Servers
  - Distribute communication for session participants
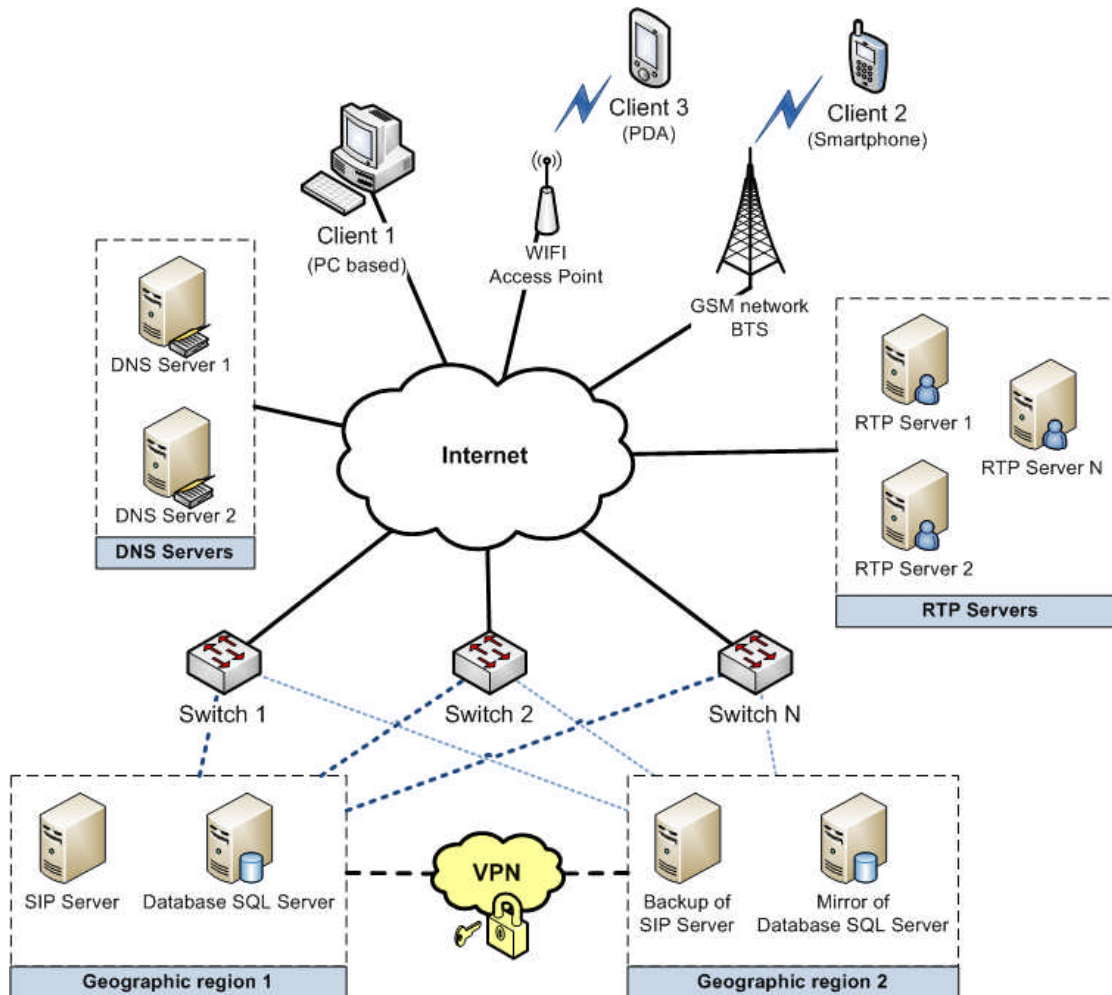
System Convergence
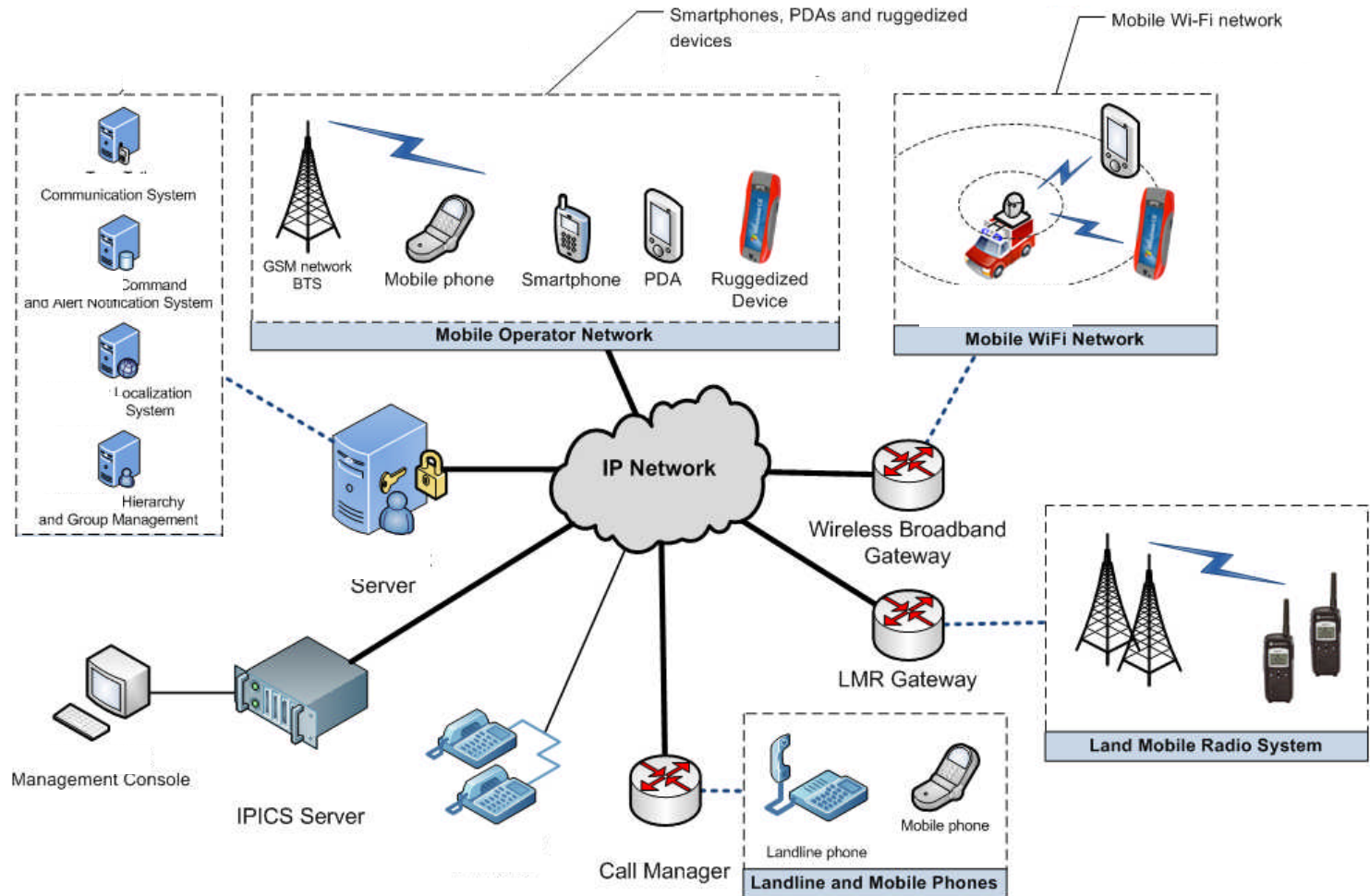
Contributions from Partners

- User Requirements

- Infrastructure

- Applications

Contact

- SECRICOM Website (www.secricom.eu)

- Presenters:

Dr A Aldabbagh
Portsdown Technology Park
QinetiQ, UK

Tel: +44 (0) 2392 31 2107
Fax: +44 (0) 2392 31 2852
E-mail: aaldabbagh@qinetiq.com

Mr J Stoodley
Portsdown Technology Park
QinetiQ, UK

Tel: +44 (0) 2392 31 2107
Fax: +44 (0) 2392 31 2852
E-mail: jastoodley@qinetiq.com

Shaun O'Neill
BAPCO
Mobile: +44 (0) 7785 925450
E-mail: euprojectofficer@bapco.org.uk

Discussion